COMMERCE, JUSTICE, SCIENCE, AND RELATED AGENCIES APPROPRIATIONS FOR FISCAL YEAR 2014

THURSDAY, MAY 16, 2013

U.S. SENATE,
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 10:02 a.m., in room SD–192, Dirksen Senate Office Building, Hon. Barbara A. Mikulski (chairwoman) presiding.

Present: Senators Mikulski, Shelby, Collins, and Boozman.

DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION

STATEMENT OF HON. ROBERT S. MUELLER, III, DIRECTOR

OPENING STATEMENT OF SENATOR BARBARA A. MIKULSKI

Chairwoman MIKULSKI. Good morning, everybody. Today the Subcommittee on Commerce, Justice, Science, and Related Agencies (CJS) will hear from the Director of the Federal Bureau of Investigation (FBI) Robert S. Mueller, III about the FBI and its budget priorities for fiscal year 2014. This process today will be in two areas: one, our open and public hearing; and then second we will move to a classified meeting to go over other aspects related to our global war against terrorism.

We want to welcome Director Mueller for his last scheduled hearing before CJS. Director Mueller will be the longest serving FBI Director since J. Edgar Hoover when he retires in September. He is the only Director to serve out a full 10-year term plus an additional two.

Director Mueller, we want to thank you for your service. We want to thank you for leading the FBI through probably one of its greatest transformations in FBI history. We want to thank you for staying an additional 2 years as we moved into a new enduring war, the cyber security aspects. We also want to thank you for being one of those nighthawk people who are always available 24–7, because that's the nature of threats that we face in our country, both here in our own country and those from around the world.

Your leadership has transformed the FBI from a domestic law enforcement agency into a global antiterrorism and anticrime police force. So while maintaining a vigorous domestic law enforcement

agency, there has also been the evolution to deal with these predatory threats.

We're going to listen to your testimony today about what we need to make sure that the FBI is the premier Federal law enforcement agency in the United States of America and, I might add, in the world. We do know that there are many eyes on the FBI right now, particularly those related to the Boston Marathon bombing. I know all of us and all at the FBI mourn what happened there. For me, four Marylanders were injured.

One, Erika Brannock, a 29-year-old preschool teacher from Trinity Episcopal, the Episcopal Children's Center in Towson, lost her leg, but she hasn't lost her spirit. She was there with her mother, her sister, and her sister's husband on that day. All the family members suffered some form of injury, but all are on the road to recovery.

But every family has a story, and we want to thank those who responded. We planned for the worst, drilled the response, and there were the coordinated law enforcement efforts.

So I know that we'll be talking; probably there will be a number of questions about that, particularly in terms of the authorities that the FBI needs to do its job, to be able to prevent such things from happening, the resources necessary to do the important work, and were there any investigatory gaps.

But you know, while all eyes are on Boston, also all eyes are on the FBI. I was just struck during the last couple of days by what the FBI has been involved with: ricin-laced letters sent to Senator Wicker and a Mississippi judge. The plant explosion in Texas, a melancholy event, was it an act of a predator or was it an accident? Those three kidnapped girls from Ohio, the FBI was involved in there. That big, $45 million ATM heist which was exposed, $45 million in an international coordinated effort. And all at the same time going after everything from other bank robbers to those who have a predatory intent to our country.

So we want to listen to the issues facing the FBI, and we are concerned about the budget. The President's request is at $8.4 billion. We know that the FBI's appropriation was enacted at $8.1 billion, but after the sequester it was $7.5 billion. We are deeply concerned that if sequester continues in fiscal year 2014, there will be an additional $700 million cut to the FBI. This is a stunning amount of money, particularly when we look at the incredible things that the FBI needs to do.

We're heartened by the fact that the President has increased the appropriations request for new major programs: one such request is $87 million for the next generation of cyber initiatives; another anticipates the need for expanding the National Instant Criminal Background Check System by requesting $100 million for new people; $7.4 million for an important biometrics technology facility in Alabama.

He has maintained support for critical programs, but they're flat-funded: counterterrorism, violent crime, fighting exploitation of children, in which I know you've been an enormous advocate, and the protection of civil rights by investigating hate crimes and the despicable practice of human trafficking. We're also concerned about the major reductions, particularly in something like elimi-

nating the National Gang Intelligence Center and the consequences of that.

So, Mr. Director, we're looking forward to hearing what the request will be, how you think it will meet important FBI needs. We also welcome you to comment on the sequester today and what the consequences to the FBI would be if sequester continues in fiscal year 2014.

PREPARED STATEMENT

I'm going to ask that my entire statement be included in the record. I now turn to my vice chairman, Senator Shelby.

[The statement follows:]

PREPARED STATEMENT OF SENATOR BARBARA A. MIKULSKI

Good morning and welcome. Today, the Commerce, Justice, Science, and Related Agencies (CJS) Subcommittee will hear from Federal Bureau of Investigation (FBI) Director Robert S. Mueller III about the FBI's budget and priorities for fiscal year 2014.

We welcome Director Mueller to his last scheduled hearing before the CJS Subcommittee. When he leaves office, he will be longest-serving FBI Director since J. Edgar Hoover, and the only Director to serve out a full 10-year term plus an additional 2 years. I thank you for your service to our Nation.

Director Mueller is one of the nighthawks, always ready for that 3 a.m. phone call. His leadership has transformed the FBI from a traditional domestic law enforcement agency into a global anti-terrorism and anti-crime police force, keeping us safe here at home from threats. I note that two national tragedies bookend Director Mueller's service. He came into this job just a week before the 9/11 terrorist attacks, and he will leave just after the Boston bombings.

Today, all eyes are on Boston. We just sustained the first terrorist attack on the United States since 9/11, with the Boston Marathon bombings. It was an attack on the Nation that has impacted all of us—including my home State. Four Marylanders were injured in the attack. "Erika Brannock is a 29-year-old teacher at Trinity Episcopal Children's Center in Towson. Erika grew up in Ellicot City and Bowie, and she sustained serious injuries to both legs and feet. Also injured was Ericka 's mother Carol Downing, who is from Monkton, Maryland. Carol ran in the marathon that day, and was taken to Brigham and Women's hospital after the bombing.

Nicole Gross is a 31-year-old personal trainer who suffered two broken legs in the bombing. She was a star swimmer at Mount Hebron High School in Ellicott City, Maryland, and now lives in Charlotte, North Carolina. And Nicole's husband, Michael Gross, who suffered lacerations and burns in the bombing.

When they were attacked and the Nation was attacked the American people responded. Thank you to the first responders who ran toward danger—the police, fire fighters, paramedics, nurses, and doctors. Working together, they saved lives and limbs.

After 9/11, we funded training and preparedness, so first responders knew and practiced where to go, what to do, and how to help. Boston was ready to respond because they planned for the worst and they drilled their response. There were well coordinated law enforcement resources—the police and the FBI—through the Joint Terrorism Task Forces.

After 9/11, FBI was charged with a new national security mission, to disrupt terrorist plots before they happen by identifying, tracking, and defeating terrorist cells and dismantling weapons of mass destruction on U.S. soil. Today, counterterrorism and counterintelligence activities make up more than 40 percent of the FBI's budget.

Boston put the focus on the FBI's counterterrorism investigations. There were immediate successes in analyzing the evidence, pouring through the video, and identifying and catching the Tsarnaev brothers.

But we also have questions about the process, things we need to know from the FBI. For instance, there appear to have been investigatory gaps. Tamerlan Tsarnaev was on the radar screen, but he slipped through the cracks. Is our system to share information on terrorist threats broken? Can it identify a lone wolf terrorist? We know that the FBI questioned Tamerlan Tsarnaev, but couldn't open a case. Does the FBI have the tools it needs to not only identify threats, but also to follow up

on those threats? Is this budget request is enough to tackle all of the counterterrorism responsibilities and keep the FBI ahead of the bad guys?

Today, all eyes are on Boston and all eyes are on the FBI. Since the Boston bombings, ricin-laced letters have been sent to the President, Senator Wicker, and a Mississippi judge. A fertilizer plant explosion in West, Texas, killed 15 and injured 200. Three women kidnapped in Cleveland, Ohio, escaped from a decade of captivity. A Minnesota pipe bomb attack was foiled in the planning stages. A $45 million ATM heist was exposed and eight criminals indicted. Top Ten Fugitive child pornographer Eric Toth, was captured in Nicaragua. And gunmen opened fire on a New Orleans Mother's Day parade.

In each case, the FBI was on the scene taking the lead or supporting other local, State, and Federal partners. We expect a lot of the FBI. We count on the FBI to keep 316 million Americans safe from terrorism and violent crime, to dismantle organized crime and drug cartels, to combat gang violence and illegal drug and gun smuggling, and to catch child sexual predators and cyber criminals.

But what should the FBI expect of us, the Congress? Rather than providing the resources to face varied and growing threats, the Congress has subjected the FBI to shutdown and showdown politics, uncertain funding, and now the sequester. Because of sequester, the FBI is operating at $543 million less than the fiscal year 2013 enacted level, and unless we end the sequester, the FBI will be cut by at least $700 million in fiscal year 2014.

We know what the FBI expects of us. They expect stable and consistent funding, so that the FBI has the resources needed to keep Americans safe. Every day, we expect the FBI to keep America safe from terrorists and criminals. The FBI expects the Congress to provide them with the resources it needs, on time and under the regular order, without shutdowns or showdowns. And that is what I intend to do as Chairwoman of the Appropriations Committee.

Once again, I thank the people of the FBI and Director Mueller for his leadership. For the information of Senators, we'll begin our examination of the FBI's $8.4 billion fiscal year 2014 budget request with this open hearing, and then we will recess at 11 a.m. and move the hearing into a classified session, where we can talk more fully about Boston and other key national security threats like cybersecurity.

STATEMENT OF SENATOR RICHARD C. SHELBY

Senator SHELBY. Thank you, Madam Chairman.

Director Mueller, we thank you for joining us here again today. You're no stranger. We also want to thank you for your service to the country.

I want to begin by also thanking the men and the women that work with you at the FBI, who work every day to protect this Nation. We're all indebted to them for the sacrifices that they and their families make.

Since the attacks of September 11, the FBI has been tasked with additional national security responsibilities. Today the FBI's mission includes, among other things, protecting the United States against acts of terror, foreign intelligence threats, cyber crime, while simultaneously maintaining focus on traditional criminal activities such as violent crime, public corruption, and white collar crime.

Criminals and terrorists are increasingly agile and sophisticated. The same is required of the FBI. The constantly changing landscape of criminal activity at home and abroad has challenged the FBI's ability to quickly respond to emerging threats. In recent years we have seen threats arise in the areas of home mortgages, financial fraud, cyber security, and of course terrorism. But it won't stop there. I believe that new, unimagined threats will challenge the FBI and all of us in the future.

To remain effective, I believe it's imperative that FBI have the inherent capability to retool and refocus to address these threats.

Without a plan to address these threats, the FBI will continue to lurch from crisis to crisis, which is something none of us want.

In the past, FBI has received additional resources from the Congress precisely because it has not been agile enough to refocus its efforts internally. This is not an effective way to address such pressing issues.

The FBI request for fiscal year 2014, Madam Chairman, says $8.3 billion. Director Mueller, while the budget request targets a number of new initiatives and maintains core missions, I believe it lacks focus on how the FBI will address future unexpected threats that I've just mentioned. Recognizing the world in which we live and the tough fiscal climate, I'm concerned that the budget priorities reflected in this request do not always ensure that the Bureau is efficient, effective, and, more importantly, nimble for the foreseeable future.

I'm committed, and I know the chairperson is, to working with you and others at what I believe are deficiencies in the budget and to budget limited resources in a manner that safeguards taxpayers while preserving public safety.

PREPARED STATEMENT

I look forward to hearing from you, Mr. Director, about the FBI's budget and its priorities. I'm also interested in hearing about the FBI's work pre- and post-Boston bombing. And finally the recent acknowledgment by the Department of Justice that they have obtained the telephone records of the Associated Press journalists has many people concerned. While I appreciate that this is an ongoing investigation, I hope that you will be as forthcoming as possible in addressing this issue here today.

Thank you, Mr. Director.

[The statement follows:]

PREPARED STATEMENT OF SENATOR RICHARD C. SHELBY

Thank you, Madame Chair.

Director Mueller, thank you for joining us today to discuss the FBI's 2014 budget request.

I want to begin by thanking the men and women of the FBI who work every day to protect this Nation. We are all indebted to them for the sacrifices they make.

Since the attacks of September 11th, the FBI has been tasked with additional national security responsibilities. Today, the FBI's mission includes protecting the United States against acts of terror, foreign intelligence threats and cyber-crime while simultaneously maintaining focus on traditional criminal activities such as violent crime, public corruption, and white-collar crime.

Criminals and terrorists are increasingly agile and sophisticated. The same is required of the FBI.

The constantly changing landscape of criminal activity at home and abroad has challenged the Bureau's ability to quickly respond to emerging threats. In recent years we have seen threats arise in the areas of home mortgages, financial fraud, cyber-security and, of course, terrorism. But it won't stop there. I believe that new, unimagined threats will challenge the FBI in the future.

To remain effective, it is imperative that the Bureau have the inherent capability to retool and refocus to address nascent threats. Without a plan to address these threats, the FBI will continue to lurch from crisis to crisis.

In the past, the Bureau has received additional resources from Congress precisely because it has not been agile enough to refocus its efforts internally. This is not an effective way to address such pressing issues.

The FBI request for 2014 is $8.3 billion. Director Mueller, while the budget request targets a number of new initiatives and maintains core missions, it lacks any

focus on how the Bureau will address the future, unexpected threats that I just mentioned.

Recognizing the world in which we live and the tough fiscal climate, I am concerned that the budget priorities reflected in this request do not ensure that the Bureau is efficient, effective and, more importantly, nimble for the foreseeable future.

I am committed to working with you and the Chair to address, what I believe are deficiencies in the budget and to target limited resources in a manner that safeguards taxpayer dollars while preserving public safety.

I look forward to hearing from you Director Mueller about the Bureau's budget and its priorities. I am also interested in hearing about the FBI's work pre- and post- the Boston bombing.

Finally, the recent acknowledgement by the Department of Justice that they have obtained the telephone records of Associated Press journalists has many of us concerned. While I appreciate this is an ongoing investigation, I hope that you will be as forthcoming as is possible in addressing the issue here today.

Thank you Madame Chair.

Chairwoman MIKULSKI. Mr. Director.

SUMMARY STATEMENT OF HON. ROBERT S. MUELLER, III

Mr. MUELLER. Thank you. Good morning, Chairman Mikulski and Ranking Member Shelby. Even though not here, I thank the other members of the subcommittee who have served over a period of time on this subcommittee. I want to thank you for the opportunity to appear here today and, on behalf of the men and women of the FBI, let me begin by thanking you, particularly you two, for your continuous support over the 11 years that we have worked together.

As pointed out, we live in a time of diverse and persistent threats from terrorists, spies, and cyber criminals. At the same time, we face a wide range of criminal threats, from white collar crime to public corruption, to transnational criminal syndicates, migrating gangs, and child predators. Just as our national security and criminal threats constantly evolve, so too must the FBI counter these threats even during a time of constrained budgets as, Senator, you have pointed out.

Today, I would like to highlight several of the FBI's highest priority national security threats. I'll start with Boston. As illustrated by that recent attack, terrorist threats against the United States remain our top priority. Over the past few weeks we have seen an extraordinary effort by law enforcement, intelligence, and public safety agencies to find and hold accountable those responsible for the Boston bombings.

As you know, one of the bombers is dead, a second suspect has been charged, and we continue our ongoing efforts to identify any others who may be responsible. The collaborative efforts of all of our partners, with the help and the cooperation of the public, have led to the results so far, and let me assure you there will be no pause in that effort.

There are limits to what we can discuss publicly about the case today, as the investigation is active and ongoing. But as this case illustrates, we face a continuing threat from home-grown violent extremists. These individuals present unique challenges because they do not share a typical profile. Their experiences and motives are often not distinct, which makes them very difficult to identify and to stop.

Yet at the same time, foreign terrorists still seek to strike us at home and abroad. Terrorists today operate in more places and

against a wider array of targets than they did a decade ago. We have seen an increase in cooperation among terrorist groups, and an evolution in their tactics and their communications. Core Al-Qaeda is weaker and more decentralized than it was 11 years ago, but it remains committed to attacks against the West.

Al-Qaeda affiliates and surrogates, in particular Al-Qaeda in the Arabian Peninsula, pose a continuing and a growing threat. In light of the recent attacks in North Africa, we must focus on emerging extremist groups capable of carrying out such additional attacks.

Next, let me turn for a second to discuss the cyber threat, which has evolved significantly over the past decade and cuts across all FBI programs. Cyber criminals have become increasingly adept at exploiting weaknesses in our computer networks, and once inside they can exfiltrate both state secrets and trade secrets. We also face persistent threats from hackers for profit, organized criminal cyber syndicates, and hacktivist groups. As I have said in the past, I believe that the cyber threat may well eclipse the terrorist threat in years to come.

In response, we are strengthening our cyber capabilities in the same way we enhanced our intelligence and national security capabilities in the wake of the September 11 attacks. The Cyber Division is focused on computer intrusions and network attacks. FBI special agents work side by side with Federal, State, and local counterparts on cyber task forces in each of our 56 field offices, working to detect and disrupt computer intrusions.

We have increased the size and the scope of the National Cyber Investigative Joint Task Force, which brings together 19 law enforcement, military, and intelligence agencies to stop current attacks and prevent future attacks. Together with the Department of Homeland Security and the National Security Agency (NSA), we have clarified the lanes in the road for our collective response to significant cyber intrusions.

Now, cyber crime, as many other crimes today, requires a global approach. In the cyber arena, through FBI legal attaché offices, we are sharing information and coordinating investigations with our international counterparts. We have special agents embedded with police departments in Romania, Estonia, Ukraine, and the Netherlands to identify emerging trends and key players. At the same time, we fully recognize that the private sector is the essential partner to protect our criminal infrastructure and to share information, threat information in particular.

Let me turn for a moment to the FBI's criminal programs. The FBI's responsibilities range from complex white collar fraud to transnational criminal enterprises and from violent crime to public corruption. Given limited resources, we must focus on those areas where we bring something unique to the table.

For example, violent crime and gang activity continue to exact a high toll on our communities. Through Safe Streets and Safe Trails Task Forces, we identify and target the most dangerous of these criminal enterprises. To track and disrupt violence along the Southwest Border, we rely on our partnerships with the Drug Enforcement Administration led Special Operations Division, the Or-

ganized Crime Drug Enforcement Task Force Fusion Center, and the El Paso Intelligence Center.

At the same time, we are required to and must remain vigilant in our efforts to find and to stop child predators. Our mission in that regard is threefold: first, to decrease the vulnerability of children to exploitation; second, to provide a rapid, effective response to crimes against children through programs such as the Child Abduction Rapid Deployment Teams; and third, to enhance the capabilities of State and local law enforcement through task force operations such as the Innocent Images and the Innocence Lost National Initiatives.

Now, in closing I would like to turn to sequestration. The impact of sequestration on the FBI's ability to protect the Nation from terrorism and crime will be significant. In fiscal year 2013, the FBI's budget was cut by more than $550 million and in fiscal year 2014, proposed cuts will total more than $700 million. This does not include the rescission in fiscal year 2013 of approximately an additional $150 million.

The ongoing hiring freeze will result in 2,220 vacancies at the FBI by the end of this fiscal year, with 1,300 additional vacancies in 2014. We also anticipate furloughs for our employees during the next fiscal year. I have long said that people are the FBI's greatest asset. Additional operational cuts and furloughs will impact the FBI's ability to prevent crime and terrorism, which in turn will impact the safety and security of our Nation.

With regard to nonpersonnel resources, the FBI will have to forego or delay long-needed IT upgrades and additionally will be unable to obtain the technical surveillance tools needed to keep pace with our adversaries.

We understand the need for budget reductions, but we would like to work with the subcommittee to mitigate the most significant impacts of those cuts.

PREPARED STATEMENT

Chairman Mikulski and Ranking Member Shelby, I personally would like to thank you again for your support to the FBI over the years that I have been Director and for your support of our office. Our transformation over the past decade would not have been possible without not only your cooperation, but your support, and for that we in the Bureau thank you.

Again, I look forward to any questions you may have.

[The statement follows:]

PREPARED STATEMENT OF HON. ROBERT S. MUELLER, III

Good morning Chairwoman Mikulski, Ranking Member Shelby, and members of the subcommittee. I look forward to discussing the Federal Bureau of Investigation's (FBI) efforts as a threat-driven, intelligence-led organization that is guided by clear operational strategies and priorities.

The FBI has established strong practices for sharing intelligence, leveraged key technologies to help us be more efficient and productive, and hired some of the best to serve as Special Agents, Intelligence Analysts, and professional staff. We have built a workforce and leadership cadre that view change and transformation as a positive tool for keeping the FBI focused on the key threats facing our Nation.

Just as our national security and criminal adversaries and threats constantly adapt and evolve, so must the FBI be able to quickly respond with new or revised strategies and operations to counter these threats. Looking forward, a key challenge

facing the FBI will be maintaining its current capabilities and capacities to respond to these threats at a time when the budgetary environment remains constrained.

We live now, and will for the foreseeable future, in a time of acute and persistent threats to our national security, economy, and community safety from terrorists, foreign adversaries, criminals and violent gangs, and cyber attackers. The attacks in Boston are vivid examples of the threat. This subcommittee understands these threats—and the consequences of failing to address them. I look forward to working with the subcommittee to ensure that the FBI maintains the intelligence, investigative, and infrastructure capabilities and capacities needed to deal with these threats and crime problems within the current fiscal climate. One lesson we have learned is that those who would do harm to the Nation and its citizens will exploit any weakness they perceive in the ability and capacity of the U.S. Government to counter their activities. We must identify and fix those gaps while not allowing new weaknesses or opportunities for terrorists, cyber criminals, foreign agents, and criminals to exploit.

The FBI's fiscal year 2014 budget request totals $8.4 billion in direct budget authority, including 34,787 permanent positions (13,082 Special Agents, 3,026 Intelligence Analysts, and 18,679 Professional Staff). This funding level provides critical funding to address threats posed by terrorists, cyber attackers, and criminals.

The threats facing the homeland, briefly outlined below, underscore the complexity and breadth of the FBI's mission to protect the Nation in a post-9/11 world. Let me briefly summarize the key national security threats and crime problems that this funding supports.

NATIONAL SECURITY THREATS

Terrorism.—We have pursued those who committed, or sought to commit, acts of terrorism against the United States. Along with our partners in the military and intelligence communities, we have taken the fight against terrorism to our adversaries' own sanctuaries in the far corners of the world—including Iraq, Afghanistan, Pakistan, Yemen, Southwest Asia, and the Horn of Africa. We have worked to uncover terrorist cells and supporters within the United States and disrupted terrorist financial, communications, and operational lifelines at home and abroad. We have built strong partnerships with law enforcement in countries around the world.

The threat from terrorism remains complex and ever-changing. We are seeing more groups and individuals engaged in terrorism, a wider array of terrorist targets, greater cooperation among terrorist groups, and continued evolution and adaptation in tactics and communication.

Threats from homegrown terrorists are also of great concern. These individuals are difficult to detect, able to connect with other extremists, and—in some instances—highly capable operationally. There is no typical profile of a homegrown terrorist; their experiences and motivating factors are distinct. Many questions remain as to the precise motivation, planning, and possible support to the attacks in Boston. However, it is increasingly likely that the Boston attacks may prove to be the latest example of homegrown extremism.

Radicalization to violence remains an issue of great concern. Many factors appear to contribute to radicalization here at home, and those factors may explain why radicalization is more prevalent now than in the past. First, American extremists appear to be attracted to wars in foreign countries. We have already seen a number of Americans travel overseas to train and fight with extremist groups. The increase and availability of extremist propaganda in English perpetuate the problem.

The Internet has had a profound impact on radicalization. It has become a key platform for spreading extremist propaganda and has been used as a tool for terrorist recruiting, training, and planning. It also serves as a means of communication for like-minded extremists.

While we have had success both in disrupting plots and obtaining convictions against numerous terrorists, we have seen more groups engage in terrorism, an evolution in terrorist tactics and means of communication, and a wider array of terrorist targets here at home. All of this makes our mission that much more difficult. Therefore, the fiscal year 2014 budget request includes 28 positions (4 Special Agents and 24 Professional Staff) and $6 million for surveillance resources to help combat International Terrorism.

Foreign Intelligence.—While foreign intelligence services continue traditional efforts to target political and military intelligence, counterintelligence threats now include efforts to obtain technologies and trade secrets from corporations and universities. The loss of critical research and development data, intellectual property, and insider information poses a significant threat to national security.

Each year, foreign intelligence services and their collectors become more creative and more sophisticated in their methods to steal innovative technology, which is often the key to America's leading edge in business. Last year alone, the FBI estimates that economic espionage cases cost the American economy more than $13 billion. In the last 4 years, the number of FBI arrests associated with economic espionage has doubled; indictments have increased five-fold; and convictions have risen eight-fold.

As the FBI's economic espionage caseload is growing, the percentage of cases attributed to an insider threat has increased, meaning that individuals trusted as employees and contractors are a growing part of the problem. The insider threat is not new, but it is becoming more prevalent for a range of reasons, including that theft of company information is a low-cost route to avoid investment in research; the ease of stealing information that is stored electronically, especially when one has legitimate access to it; and the increasing exposure of businesses to foreign intelligence services as joint ventures grow and businesses become more global.

To address the evolving insider threat, the FBI has become more proactive to prevent losses of information and technology. The FBI continues expanding outreach and liaison alliances to Government agencies, the defense industry, academic institutions, and, recently, to the general public, because of an increased targeting of unclassified trade secrets across all American industries and sectors.

Through these relationships, the FBI and its counterintelligence partners must continue our efforts to identify and prevent the loss of sensitive American technology.

Intelligence.—Since September 11, 2001, we have improved our intelligence collection and analytical capabilities. Today, we are collecting and analyzing intelligence to better understand all threats—those we know about and those that have not yet materialized. We recognize that we must always look for ways to refine our intelligence capabilities to stay ahead of these changing threats. The FBI recently restructured its Directorate of Intelligence to maximize organizational collaboration, identify and address emerging threats, and more effectively integrate intelligence and operations within the FBI. With this new structure, each office can better identify, assess, and attack emerging threats.

Cyber.—As this subcommittee knows, the cyber arena has significantly changed over the last decade. Cyber attacks and crimes are becoming more commonplace, more sophisticated, and more dangerous. The scope and targets of these attacks and crimes encompass the full range and scope of the FBI's criminal investigative and national security missions. Traditional crime, from mortgage and health care fraud to child exploitation, has migrated online. Terrorists use the Internet to recruit, to communicate, to raise funds, to train and propagandize, and as a virtual town square, all in one. On a daily basis, we confront hacktivists, organized criminal syndicates, hostile foreign nations that seek our state secrets and our trade secrets, and for profit actors willing to hack for the right price.

Since 2002, the FBI has seen an 84-percent increase in the number of computer intrusions investigations. Hackers—whether state sponsored, criminal enterprises, or individuals—constantly test and probe networks, computer software, and computers to identify and exploit vulnerabilities. We are working with our partners, both foreign and domestic, to develop innovative ways to identify and confront the threat as well as mitigate the damage. There is always more work to be done, but we have had some success, including the 2011 takedown of Rove Digital, a company founded by a ring of Estonian and Russian hackers to commit a massive Internet fraud scheme.

The Rove Digital scheme infected more than four million computers located in more than 100 countries with malware. The malware secretly altered the settings on infected computers, enabling the hackers to digitally hijack Internet searches using rogue servers for Domain Name System (DNS) routers and re-routing computers to certain websites and ads. The company received fees each time these Web sites or ads were clicked on or viewed by users and generated $14 million in illegitimate income for the operators of Rove Digital.

We were able to work with our law enforcement counterparts in Estonia and our private industry partners to take down this criminal organization. Following the arrest of several co-conspirators in Estonia, teams of FBI agents, linguists, and forensic examiners assisted Estonian authorities in retrieving and analyzing data that linked the co-conspirators to the Internet fraud scheme. At the same time, we obtained a court order in the United States to replace the rogue DNS servers with court-ordered clean servers.

In this case, we not only took down the criminal organization, but we also worked with our partners in the Department of Homeland Security (DHS) and other agencies to mitigate the damage. Seven individuals have been indicted in the Southern

District of New York in this case: six in Estonia and one in Russia. The United States has sought extradition of all six Estonian subjects. To date, two of them have been remanded to U.S. custody, and both have pleaded guilty.

We have also worked against infrastructure we believe has been used in Distributed Denial of Service (DDOS) attacks, preventing it from being used for future attacks. Since October, the FBI and the Department of Homeland Security (DHS) have released nearly 168,000 Internet Protocol (IP) addresses determined to be infected with DDOS malware. We have released this information through Joint Indicator Bulletins (JIBs) to 129 countries. Both the DHS' Computer Emergency Readiness Team (CERT) and FBI's Legal Attaches released JIBs to our foreign partners. These actions have enabled our foreign partners to take action and reduced the effectiveness of the botnets and the DDOS attacks.

Just as the FBI has transformed its counterterrorism and intelligence programs to deal with an evolving and adapting threat, the Bureau is strengthening its cyber program and capabilities. Computer intrusions and network attacks are the greatest cyber threat to our national security. To better prioritize our cyber resources on the greatest cyber threats, last year we focused our Cyber Division on computer intrusions and moved all other cyber-facilitated crimes that are perpetrated over the Internet to our Criminal Investigative Division.

The FBI has also focused on hiring specialized personnel to address this growing threat. The FBI now has more than 1,000 specially trained agents, analysts, and digital forensic examiners that run complex undercover operations and examine digital evidence. The FBI is also the executive agent of the National Cyber Investigative Joint Task Force, which includes representatives from 19 law enforcement and intelligence agency partners. The task force operates through Threat Focus Cells—smaller groups of agents, officers, and analysts focused on particular threats.

Both the Cyber Division and the NCIJTF are increasingly engaging the private sector in our effort to combat cyber threats. We distribute cyber threat information to victim companies, sometimes permitting them to stop cyber attacks before they happen. Appropriate two-way dialogue with the private sector is essential for the FBI to engage in time-sensitive investigative and disruption activities, including determining whether the cyber threat poses a threat to national security.

U.S. law enforcement and intelligence communities, along with our international and private sector partners, are making progress. Technological advancements and the Internet's expansion continue to provide malicious cyber actors the opportunity to harm U.S. national security and the economy. Given the consequences of such attacks, the FBI must be able to keep pace with this rapidly developing and diverse threat. Because of this, the fiscal year 2014 budget request includes an additional 152 positions (60 Special Agents, 1 Intelligence Analyst, and 91 Professional Staff) and $86.6 million to help address this threat.

TEDAC.—The FBI established the Terrorist Explosive Devices Analytical Center, or TEDAC, in 2003. Over the past 10 years, it has proved to be a valuable tool supporting the military, homeland security, international partners, intelligence, and law enforcement communities. Prior to TEDAC, no single part of our Government was responsible for analyzing and exploiting intelligence related to terrorist Improvised Explosive Devices (IEDs). Today, TEDAC supports the efforts of our entire Government, from law enforcement to intelligence to the military, in developing and sharing intelligence about terrorist explosive devices.

Nearly all IEDs of interest to the United States Government pass through TEDAC, allowing our technicians, examiners, scientists, and intelligence analysts to see the full spectrum of devices and to recognize trends in their construction and components. TEDAC was (and remains) responsible for analyzing the devices used in the recent Boston attacks. This, in turn, helps us to disarm or disrupt these devices; to link IEDs to their makers; to develop new countermeasures and most importantly, to prevent future attacks.

TEDAC has received more than 95,000 submissions since its creation. By forensically and technically exploiting IEDs and their components, scientists and engineers are able to make matches and connections between seemingly unrelated IEDs. These connections have supplied valuable information to our war fighters on the front lines, as well as law enforcement and intelligence personnel protecting the homeland. TEDAC's work has resulted in actionable intelligence and progress in the fight against increasingly sophisticated and deadly explosive devices.

Thanks to the resources provided by this committee the FBI has begun construction of a new TEDAC facility at Redstone Arsenal in Huntsville, Alabama which is expected to be complete by February 2014. This new facility will allow TEDAC operations to be collocated at a single site, allowing for more efficient and integrated forensic and intelligence activities.

CRIMINAL THREATS

The Nation faces many criminal threats, from complex white-collar fraud in the financial, health care, and housing sectors to transnational and regional organized criminal enterprises to violent gangs and crime to public corruption. These threats have also changed significantly since 2002. Criminal organizations—domestic and international—and individual criminal activity represent a significant threat to our security and safety in communities across the Nation. I would like to briefly highlight a number of these criminal threats and FBI capabilities for addressing these threats.

Gangs and Violent Crime.—Violent crimes and gang activities exact a high toll on individuals and communities. There are approximately 33,000 violent street gangs, motorcycle gangs, and prison gangs with about 1.4 million members active in the U.S. today. A number of these gangs are sophisticated and well organized; many use violence to control neighborhoods and boost their illegal money-making activities, which include robbery, drug and gun trafficking, fraud, extortion, and prostitution rings. Gangs do not limit their illegal activities to single jurisdictions or communities. FBI is able to work across such lines, which is valuable to the fight against violent crime in big cities and small towns across the Nation. Every day, FBI Special Agents work in partnership with State and local officers and deputies on joint task forces and individual investigations.

FBI joint task forces—Violent Crime Safe Streets, Violent Gang Safe Streets, and Safe Trails Task Forces—focus on identifying and targeting major groups operating as criminal enterprises. Much of the Bureau's criminal intelligence is derived from our State, local, and tribal law enforcement partners, who know their communities inside and out. Joint task forces benefit from FBI surveillance assets and its sources track these gangs to identify emerging trends. Through these multi-subject and multi-jurisdictional investigations, the FBI concentrates its efforts on high-level groups engaged in patterns of racketeering. This investigative model enables us to target senior gang leadership and to develop enterprise-based prosecutions.

Violence Along the Southwest Border.—Violence and corruption associated with drug trafficking in Mexico continues to be a significant issue—not only along the Southwest Border, but in many communities throughout the United States where Mexican drug traffickers have established a presence. In addressing this crime problem, the FBI relies on a multi-faceted approach for collecting and sharing intelligence—an approach made possible and enhanced through the Southwest Intelligence Group, the El Paso Intelligence Center, OCDETF Fusion Center, and the Intelligence Community. Guided by intelligence, the FBI and its Federal law enforcement partners are working diligently, in coordination with the government of Mexico, to counter violent crime and corruption that facilitates the flow of illicit drugs into the United States.

Organized Crime.—Ten years ago, the image of organized crime was of hierarchical organizations, or families, that exerted influence over criminal activities in neighborhoods, cities, or States. But organized crime has changed dramatically. Today, international criminal enterprises run multi-national, multi-billion-dollar schemes from start to finish. These criminal enterprises are flat, fluid networks and have global reach. While still engaged in many of the "traditional" organized crime activities of loan-sharking, extortion, and murder, new criminal enterprises are targeting stock market fraud and manipulation, cyber-facilitated bank fraud and embezzlement, identify theft, trafficking of women and children, and other illegal activities. This transformation demands a concentrated effort by the FBI and Federal, State, local, and international partners to prevent and combat transnational organized crime.

The FBI is expanding its focus to include West African and Southeast Asian organized crime groups. The Bureau continues to share intelligence about criminal groups with our partners, and to combine resources and expertise to gain a full understanding of each group. To further these efforts, the FBI participates in the International Organized Crime Intelligence Operations Center (IOC–2). This center serves as the primary coordinating mechanism for the efforts of nine Federal law enforcement agencies in combating non-drug transnational organized crime networks.

Crimes Against Children.—The FBI remains vigilant in its efforts to remove predators from our communities and to keep our children safe. Ready response teams are stationed across the country to quickly respond to abductions. Investigators bring to this issue the full array of forensic tools such as DNA, trace evidence, impression evidence, and digital forensics. Through improved communications, law enforcement also has the ability to quickly share information with partners throughout the world and our outreach programs play an integral role in prevention.

The FBI also has several programs in place to educate both parents and children about the dangers posed by violent predators and to recover missing and endangered children should they be taken. Through our Child Abduction Rapid Deployment teams, Innocence Lost National Initiative, Innocent Images National Initiative, Office of Victim Assistance, and numerous community outreach programs, the FBI and its partners are working to make our world a safer place for our children.

Financial and Mortgage Fraud.—From foreclosure frauds to sub-prime scams, mortgage fraud is a serious problem. The FBI continues to develop new approaches and techniques for detecting, investigating, and combating mortgage-related fraud. Through the use of joint agency task forces and working groups, the FBI and its partners work to pinpoint the most egregious offenders and identify emerging trends before they flourish. In fiscal year 2012, these efforts translated into roughly 2,265 pending mortgage fraud investigations—compared to approximately 700 investigations in fiscal year 2005. More than 70 percent of FBI's pending investigations involve losses of more than $1 million. In addition, in fiscal year 2012, the FBI received more than 70,000 Suspicious Activity Reports. The number of FBI Special Agents investigating mortgage fraud cases has also increased from 120 in fiscal year 2007 to 260 Special Agents in fiscal year 2012. The multi-agency task force and working group model serves as a force-multiplier, providing an array of interagency resources and expertise to identify the source of the fraud, as well as finding the most effective way to prosecute each case, particularly in active markets where fraud is widespread.

The FBI and its law enforcement partners also continue to uncover major frauds, insider trading activity, and Ponzi schemes. At the end of fiscal year 2012, the FBI had almost 2,500 active corporate and securities fraud investigations, representing a 35 percent increase since fiscal year 2008. Over the past 3 years, as a result of the FBI's efforts, the Department of Justice has obtained more than $20 billion in recoveries, fines, and restitutions in such programs, and during fiscal year 2012, the FBI obtained more than 600 convictions, just shy of the historic high obtained in fiscal year 2011. The FBI is pursuing those who commit fraud at every level and is working to ensure that those who played a role in the recent financial crisis are brought to justice.

In fiscal year 2014, the FBI is requesting a program increase totaling $15 million and 44 positions (40 Special Agents and 4 Forensic Accountants) to further address financial and mortgage fraud at all levels of organizations—both senior executives and lower level employees. These resources will increase the FBI's ability to combat corporate fraud, securities and commodities fraud, and mortgage fraud, and they will enable the FBI to adapt as new fraud schemes emerge.

National Instant Criminal Background Check System (NICS).—For over a decade, the FBI has been responsible for determining a person's eligibility to possess a firearm at the point of purchase from a Federal Firearms Licensees. The number of checks has grown over 200 percent since NICS was implemented in 1998. Since the tragic shooting at Sandy Hook Elementary school on December 14, 2012, and subsequent discussions of potential changes in gun laws, the FBI's workload has skyrocketed. Before the shooting, the busiest week in NICS history was the week of December 3–9, 2012, when 527,095 firearms checks were initiated. The week following the shooting, December 17–23, 2012, NICS volumes approached 1 million transactions, and continue to exceed historical peak volume. In fact, the first 6 full weeks in 2013 are among the top ten busiest weeks in NICS history. Because of this increased workload, the FBI has required NICS personnel to cancel all leave, work mandatory overtime shifts, forego other critical tasks, such as appeals and audits, and has shifted personnel from other program areas to provide assistance. Without a permanent addition to personnel, facility space, and technology improvements, national security and public safety are at risk, as the current FBI staff will be unable to provide timely and accurate determination of a person's eligibility to possess firearms and/or explosives in accordance with Federal law. Therefore, the fiscal year 2014 budget requests 524 positions and $100 million to increase the ability to process mandated background checks for firearm purchases.

TECHNOLOGY

As criminal and terrorist threats become more diverse and dangerous, the role of technology becomes increasingly important to our efforts. We are using technology to improve the way we collect, analyze, and share information. We have seen significant improvement in capabilities and capacities over the past decade; but technology remains a key concern for the future.

For example, in 2011, we deployed new technology for the FBI's Next Generation Identification System. This technology enables us to process fingerprint transactions

much faster and with more accuracy. The fiscal year 2014 budget includes $7.4 million for the facility built to partner with the Department of Defense's (DOD) Biometrics Fusion Center, which will advance centralized biometric storage, analysis, and sharing with State and local law enforcement, DOD, and others. In addition, throughout the Bureau, we are also integrating isolated stand-alone data sets so that we can search multiple databases more efficiently, and, in turn, pass along relevant information to our partners.

The FBI shares information electronically with partners throughout the Intelligence Community, across the Federal Government, as well as with State and local agencies. For example, the FBI works closely with the nationwide suspicious activity reporting (SAR) initiative to implement technical and business processes that enable the eGuardian system and the Information Sharing Environment's Shared Space system to share SARs more quickly and efficiently. These efforts have worked to ensure that SARs entered into Shared Space are simultaneously shared with eGuardian, and in turn, delivered to the appropriate Law Enforcement and Intelligence Community partners.

Sentinel, the FBI's next-generation information and case management system, was deployed to all employees on July 1, 2012. Sentinel moves the FBI from a paper-based case management system to a digital system of record. It enhances the FBI's ability to link cases with similar information through expanded search capabilities and to share new case information and intelligence more quickly among Special Agents and Intelligence Analysts. It also streamlines administrative processes through "electronic workflow." The FBI will continue refining and deploying additional Sentinel features according to employee feedback and organizational requirements.

The rapid pace of advances in mobile and other communication technologies continues to present a significant challenge to conducting court-ordered electronic surveillance of criminals and terrorists. These court-ordered surveillances are often critical in cyber cases where we are trying to identify those individuals responsible for attacks on networks, denial of services, and attempts to compromise protected information. However, there is a growing and dangerous gap between law enforcement's legal authority to conduct electronic surveillance, and its actual ability to conduct such surveillance. Because of this gap, law enforcement is increasingly unable to gain timely access to the information it needs to protect public safety and bring these criminals to justice. We are grateful for this subcommittee's support in funding the National Domestic Communications Assistance Center, which just opened its doors last month. The center will enable law enforcement to share tools, train one another in modern intercept solutions, and reach out to the communications industry with one voice.

It is only by working together—within the law enforcement and intelligence communities, and with our private sector partners—that we will find a long-term solution to this growing problem.

OFFSETS

The FBI's fiscal year 2014 budget request proposes offsets totaling approximately $61 million. Proposed offsets include: elimination of the National Gang Intelligence Center; reduction of one training day and equipment provided for specialized response team training; reduction of contractor workforce funding; reductions in funding for permanent change of station transfers; reducing funding for information technology, facilities, and other administrative initiatives; reducing funding by converting contractor positions to Government employees; and reducing security clearance funding for State and local task force officers. We will work to minimize the impact of these proposed reductions.

CONCLUSION

Responding to this complex and ever-changing threat environment is not new to the FBI. The resources this subcommittee provides each year are critical for the FBI to be able to address existing and emerging national security and criminal threats.

Chairwoman Mikulski, Ranking Member Shelby, and members of the subcommittee, I would like to close by thanking you for this opportunity to discuss the FBI's priorities. Madam Chairwoman, let me acknowledge the leadership that you and this subcommittee have provided to the FBI. The transformation the FBI has achieved would not have been possible without your support. Your investments in our workforce, our technology, and our infrastructure make a difference every day at FBI offices in the United States and around the world, and we thank you for that support.

I look forward to any questions you may have.

Chairwoman MIKULSKI. Thank you very much, Director, for your testimony. I anticipate that other members will be joining the subcommittee, but all of our appropriations subcommittees are holding hearings today, so everybody's spread a bit thin.

SEQUESTRATION

I want to go to the impact of the reduction that the FBI had to spend from fiscal year 2013, a reduction to $8.1 billion, and then with sequester even more. Let me go to both the consequences of sequester—your request—then the consequences of sequester in fiscal years 2013 and 2014. We were already in a tight budget before sequester.

Mr. MUELLER. Yes.

Chairwoman MIKULSKI. You already faced a reduction.

Mr. MUELLER. But—yes.

Chairwoman MIKULSKI. Go ahead.

Mr. MUELLER. I was going to say, yes, but in response to one or more of the comments that Senator Shelby made in terms of being a nimble FBI and to continuously reprioritize, I would say that early on, we recognized the necessity for doing that. We moved from a system where our metrics were how many arrests, indictments, and convictions we had to what is the threat out there and what has been the impact on that particular threat, and if that threat has been addressed, then let's move on to something else.

The fact of the matter is that we've got two components where we cut. One is our people, which is a last resort. We're not like the military with aircraft carriers and ships and all the rest of that stuff. We have our people.

The other part of it is the infrastructure that gives us the ability to work as an intelligence and a law enforcement agency. We protect our people. When the cuts come, it comes in other areas that are tremendously important to us, but are second to our people. So, as we address the cuts in fiscal years 2013 and 2014, we will have to reprioritize to meet the cuts. But there will be things, as I pointed out in my statement, that we will not be able to do that would keep us on track with what we've been able to accomplish the last 11 years.

IT INFRASTRUCTURE

Chairwoman MIKULSKI. Let's go to that. It says that, first, the tools of technology, whether it's cyber, biometrics aspects we support. The technology that goes on in the great laboratories you have at Quantico of course are one thing. But the FBI is known through its agents and it's literally the agents on the ground, also working with State and local law enforcement.

So what will be the impact of the hiring freeze and what do you anticipate that you will not be able to do as you prioritize? In other words, what falls off?

Mr. MUELLER. There are a number of things that fall off the list, one of them being the National Gang Intelligence Center, which has been in operation for a number of years. They centralize gang intelligence, which is critically important around the country. We will have to centralize that, disband that initiative, and try to rep-

licate many of its attributes with personnel assigned from headquarters.

We will be losing several million dollars in the Critical Incident Response Group, specifically the hostage rescue team (HRT). They have been very active recently not only in Boston, but in Alabama, with the boy who was taken off a bus and kept underground. It was the hostage rescue team that was the entity, along with the State and local authorities, that were able to resolve that particular situation.

And we'll have to cut back on Critical Incident Response Group training and capabilities. We'd also have to cut down on personnel transfers. We also have facilities reductions. We have 400 resident agencies around the country and we're going to have to look at reducing those and seeing if we can combine some of them. But those resident agencies give us the capabilities of responding anyplace in the country to a substantial Federal crime.

Those are just some of the things that will be impacted by these budget cuts.

Chairwoman MIKULSKI. Well, it seems to me, with the challenges you're facing and the management endeavors to deal with the consequences, that the threats and the needs don't go away, and we're going to make do, but this is not like deferring maintenance on a dorm somewhere. This is actually primarily personnel. Personnel needs the most up-to-date IT, what we've already been talking about, the watch list. We can go into detail about that in another setting.

But my concern is that, yes, the people are the greatest asset, exactly what Senator Shelby and I feel, our high regard for the agents. I can just tell you how highly regarded the FBI is in Maryland. We're home to premier programs like Innocent Images that protect children on the Internet. But also the day to day work of the FBI and the way they work with the Joint Task Force, the way they work with our U.S. Attorney. We have this integrated effort to protect the people of Maryland against everything from mortgage fraud to counterfeit drugs that are coming in, where you're working with the Customs people, local law enforcement. Again, these joint task forces seem so crucial, and the threats come in at the local level, except where you're talking about the big international stuff.

My concern is that this will have a chilling effect on morale. I know your agents, many of them personally, are very duty driven, very duty driven, but still it will have an effect. And it has an effect on our effectiveness at the State and local level. Do you concur with that?

Mr. MUELLER. I concur, absolutely, and particularly if we have to go to furloughs. There's nothing more—how do you want to put it? "Devastating" is perhaps too strong a word, but "demoralizing" is the word I'm looking at—as demoralizing, when you are faced with furloughs, unable to pay your bills, working hard, but the Government has to furlough you because there is insufficient money to keep you on in the position that you hold.

We take cuts elsewhere, but the furloughs is the last resort.

Chairwoman MIKULSKI. Would you anticipate that agents would be furloughed?

Mr. MUELLER. Yes. My belief is that it's very difficult to——

Chairwoman MIKULSKI. That's shocking. I've got to tell you, this is shocking, and it is incumbent—this is a self-inflicted wound. I'm going to turn to Senator Shelby in a second. This is a self-inflicted wound on us. This is not what an external threat from a foreign country or organized crime is doing to us. It's what we're doing to ourselves.

I think we have to find a solution to canceling sequester, not better managing sequester, for both this year and the next ten, because I think that's really the ultimate corrosive effect.

Let me turn to Senator Shelby.

BOSTON MARATHON BOMBING

Senator SHELBY. Thank you, Madam Chairman.

Director Mueller, last month Boston, as you well know, was the target of a terrorist attack that killed three people and wounded more than 260. I want to first of all commend the work of the FBI and the people of the FBI and the State and local law enforcement for the response to that incident. They did an exemplary job, I thought.

I'm troubled, however, by reports—and a lot of people have been—that the danger posed—and I hope I get his name right—Tamerlan Tsarnaev is close to it, I guess—was not identified because the Government again was unable to connect the dots. We've talked about this before in the intelligence area.

It's disappointing sometimes that, after 12 years and hundreds of billions of dollars in investments, we're still discussing the Government's inability at times to connect the dots when it's very important. Would you walk us through what you can here what the FBI knew about Tsarnaev and what action it took and why it did not take further action after learning that he had traveled to Russia?

And while I understand the FBI contends that it was not aware that he left the country, the Boston Globe has reported that the watch list system generated an automatic notification to an officer in the Joint Terrorism Task Force (JTTF) in Boston. Are you aware of that report?

Mr. MUELLER. Yes, Sir.

Senator SHELBY. Do you agree or disagree with the report?

Mr. MUELLER. If you're talking about the Boston Globe report——

Senator SHELBY. Yes.

Mr. MUELLER [continuing]. I'm not specifically aware of the Boston Globe report. I understand what they are addressing in terms of the text notification that went out on the travel.

Senator SHELBY. Well, what about, if the JTTF—and they didn't—had received this information, what action could they have taken based on the FBI's previous inquiry regarding this subject? I know it's——

Mr. MUELLER. Let me start, if I can——

Senator SHELBY. Yes, walk us through it, if you can.

Mr. MUELLER. To a certain extent, I can walk you through maybe 75 percent of it in open session.

Senator SHELBY. What you can.

Mr. MUELLER. But the balance we can cover in closed session.

In approximately March 2011, we received notification from the Russian authorities that an individual who I'll call Tamerlan—who is the older brother—and his mother had appeared to be very religious and, at least as far as the older brother was concerned, intent on returning and perhaps participating in jihad in Russia. They passed this information on to us to follow up on.

We initiated an assessment. An agent was assigned and the agent, a very good agent, I might add, undertook efforts to look into the background of Tamerlan. He visited the college where he had been registered for a period of time; did a thorough background on him; interviewed the parents; and finally interviewed Tamerlan himself.

As a result of this, I would say we conducted a thorough investigation based on the leads that we got from the Russians, and we found no ties to terrorism. Later that summer, in August, we got back to the Russians and indicated we did not find any ties.

Then in October, I think it was, we also went back to the Russians—on three occasions we went back to the Russians and asked them if they had any further information that would educate us or elaborate for us their concerns about this individual, but we got no response. So that assessment was closed without any further information.

But what you referred to is the travel that Tamerlan took in January through July 2012, where the Russians had asked to be notified if he was traveling. A what they call a tecs notice had gone to a very good Customs agent on the Joint Terrorism Task Force. We do not have any action that was taken on that particular notification.

Likewise, when he returned to the United States, there was an automatic message that was pushed out, and that also came to the task force in that way. There was no additional action taken on that. It may well have been because of the numerous inquiries that we handle. That particular JTTF, in any given year, handles hundreds of similar assessments, leads, and the like. To the extent that we go back and review what we could have done better, this is an area where we are looking at it, scrubbing and doing better.

I will tell you, on the other hand, that I do think that we have improved our systems tremendously since September 11. You can almost be assured that in any event there is somebody, that may have participated, had discussions, or what have you, about terrorist events, they may well have come across our radar screens. We may not have had sufficient information from a variety of sources to be able to confirm that through.

You also have occasions where persons who at one point in time appear not to be radicalized, but very quickly thereafter, after they're off your radar screen, become radicalized, and you could not have anticipated that they would undertake an attack such as we saw in Boston.

Senator SHELBY. Of course, we don't know because some people fall through the cracks. No system is perfect, yours or ours, anything. But some people point that out as a lost opportunity. Maybe we'll learn from it. Maybe the Bureau will.

Mr. MUELLER. Yes.

Senator SHELBY. In April, the Boston Herald reported that the Commonwealth Fusion Center was unaware that the FBI interviewed Tamerlan Tsarnaev as part of an investigation after the Russian agents that you talked about alerted United States officials to his increasing radicalization. It's my understanding, Mr. Director, that these entities are supposed to serve as clearinghouses for information about potential threats, and that the fusion centers content that they are charged with helping to connect the dots.

Given that the FBI is responsible for the oversight of fusion centers, how would you characterize their role with respect to intelligence-gathering, analysis, and dissemination? And is it their responsibility, the fusion centers, to connect the dots, and if so how? In other words, you're sharing information here, and I know it's difficult.

Mr. MUELLER. Let me start by saying we do not supervise the fusion centers.

Senator SHELBY. You don't. Who does?

Mr. MUELLER. The Department of Homeland Security.

Senator SHELBY. Okay.

Mr. MUELLER. But we work very—even though we do not have——

Senator SHELBY. You work with them, but you don't—you're not their supervisor.

Mr. MUELLER. We are not.

Senator SHELBY. Okay.

Mr. MUELLER. We work very closely with them. I will tell you that in Boston we have the JTTF, the fusion centers, and the various State entities with whom we have a very close sharing relationship. If you talk to the persons who are participating in these, they would be very vocal in terms of how well we work together, which was exemplified in the response to the bombing on April 15.

There was a question raised in testimony by one of the chiefs of police in Boston about his knowledge of the interview with Tamerlan. The fact of the matter is that the JTTF has State and local law enforcement personnel on every one of those task forces. I think it's something close to——

Senator SHELBY. It makes a lot of sense to have that, doesn't it?

Mr. MUELLER. It does, and that's exactly what we want. I would say perhaps 40 percent, maybe more, of task force personnel around the country are State and local law enforcement.

Now, what that JTTF and fusion center does is take in myriad threats—hundreds over a period of time—and goes through them in the same way we went through this particular threat. Others on the task force may participate in some way or shape, but because it was closed, it was not serious enough to be taken up to the leadership. In other words, you wouldn't take it up to the chief of police or the head of the FBI office when it has been closed with a finding of no association with terrorism.

So to the extent that this is pushed up as being indicative of broken relationships, to the contrary. I think if you talk to anybody in the Boston Task Force, fusion center, State police, or Boston police, I think they would say that the relationship and the sharing is excellent.

Senator SHELBY. But we still have to continue to work on sharing of information with our law enforcement people, don't we?

Mr. MUELLER. Absolutely.

Senator SHELBY. We've come a long way in the last—since you've been the Director. We've gone through that on the Intelligence Committee and in this subcommittee for years and years, and I know it's a challenge for you. It's a challenge for the CIA. It's a challenge for NSA, and Homeland Security. But the more you can work, fuse, and share, the safer we're going to be; aren't we?

Mr. MUELLER. Absolutely. I will tell you that in every one of these incidents we go back and look and say, what could we have done better? In this particular incident, handling the tecs notice is an area that we're going to do better on the next time.

IMPROVISED EXPLOSIVE DEVICES

Senator SHELBY. Let me get into another area, because this is in the Boston area, but it's highlighted. That's improvised explosive devices (IEDs), which we all see so much of because of our troops and so forth. But they've come to America now.

The Boston bombing highlighted what our troops have been encountering for years overseas, the devastation caused by improvised explosive devices, or IEDs. The threat from IEDs here, Mr. Director—you've talked about this here before—is widely recognized and in February the White House released a report on the threat and established a new task force.

In spite of the spotlight the administration placed on understanding and countering IEDs, we know it's very complicated and challenging. This budget request before us fails to prioritize funding for the terrorist explosive device, we call it TEDAC. However, I believe TEDAC is essential to our understanding of IEDs and the overall war, which is coming to this country. It certainly proved important immediately following the bombings in Boston.

Does the fiscal year 2014 budget request ensure that TEDAC has sufficient resources necessary to complete its new facility and make substantial progress on the existing backlog? And how will the $150 million rescission requested in the FBI's budget impact TEDAC, if it does at all, and could you detail that for us?

Is that too much?

Mr. MUELLER. No.

Senator SHELBY. Not for you, it isn't too much.

Mr. MUELLER. No. I think I can break it down.

Let me first talk about TEDAC and its relationship and its utility during the Boston crisis. Immediately upon the explosions, we had in Boston our bomb techs out there with the bomb techs from State police and the others. We thereafter flew fragments of the bombs to our laboratory in Quantico, where they were analyzed by TEDAC.

Very quickly, and by "very quickly" I mean within 24 to 48 hours, we had identified the mechanisms, the containers, the kind of black powder and the like that were utilized, and were then tracing the various components, such as the pressure cookers, to determine who had purchased them where.

The TEDAC bomb technicians served three roles during this period of time. A number of them were on scene—I think there were

about five that were on scene—helping pull together the fragments. They then put together intelligence bulletins to provide the intelligence to others around the country as to what was seen, in hopes that we would not see another one, but that if we did, someone would have an understanding of the device that was used.

The third area was the examination and tracing of the particular components. This was done by TEDAC staff.

Now, the future of TEDAC, as you well know, is the facility down on Redstone Arsenal which is fully financed through next year. At the end of 2014, it should house TEDAC. The issues that are outstanding relate to operation and maintenance and the necessity for maintaining this capability.

Let me address one last thing you mentioned. That is the backlog of reviewing the IEDs that have been forwarded to us from Iraq and Afghanistan. We have a very large database of such IEDs that provide intelligence to the military day in and day out, as well as law enforcement and the intelligence community around the world.

We have used that backlog to identify individuals—by fingerprints, DNA, or the method of construction of the bombs—who may have been trying to get into the United States or appear to be terrorists trying to get into other countries, whether it be in Europe or elsewhere. But we have a backlog of devices that we picked up over the years that we're trying to run through.

In order to continue that process, we need additional funds to run through that backlog. Again this is one of the things where we prioritize. With sequestration and the fiscal year 2014 budget, we'll have to cut back substantially in terms of our ability to address that backlog.

Senator SHELBY. But TEDAC should be a priority, considering the threat in this country.

Mr. MUELLER. Yes.

Senator SHELBY. Should it?

Mr. MUELLER. Yes.

Senator SHELBY. Thank you, Madam Chairman, for your indulgence.

FBI FURLOUGHS

Chairwoman MIKULSKI. Picking up on what Senator Shelby was asking, because my first line of questions was about what we would call the focusing on the local law enforcement, the criminal aspects, work locally, but these are national crimes, like mortgage fraud.

But turning to the issues related to terrorism and counterterrorism, and this goes to what you need. For the Boston bombing, the first thing was to catch the bad guys, so there had to be a tremendous mobilization of law enforcement, which meant the FBI was involved, because my first questions, I'm sure your first questions, the agents on the ground and the Boston law enforcement, was, number one, is this it? Are they planning more attacks around Boston? Who are these people? Are they part of a larger conspiracy, perhaps connected to Al-Qaeda or Al-Qaeda-inspired? And is the conspiracy in Boston? Is it going to occur in other parts of the United States? There were other marathons coming up, international events. I believe it was the London Marathon.

So the FBI had a major role because of what had happened. One, all the resources, technical as well as law enforcement, but also your role I'm sure was called up to function internationally about—first of all nationally, was this going to be part of a larger threat? And we don't want to go around canceling events and canceling marathons, etcetera.

So my question was, everything had to be—you can't dial up an agent. In other words, in order to be effective you have to have the right agents in the right place doing the right thing with the right relationships; am I correct?

Mr. MUELLER. Yes.

Chairwoman MIKULSKI. And aren't relationships developed over time, and if these agents are furloughed, if there is a hiring freeze, it would have an impact on that, am I correct?

Mr. MUELLER. Absolutely, absolutely.

Chairwoman MIKULSKI. What would have happened in Boston if we had been under furloughs? I mean, there were many things that worked very well in Boston and there are areas that are going to require revisiting and reform. I think you would agree with that.

Mr. MUELLER. I can tell you that, furlough or no furlough, everybody would have been there immediately, even if they didn't get paid, on something like that.

But the point that you make in terms of getting the right people in the right place is not accurate just for the FBI, but for the relationships with State and local law enforcement. You're familiar with the incident down in Alabama. It's having our hostage negotiators working with the sheriff and the district attorney down there. The hostage rescue team brings those elements that are important to that particular case which is not one we could have prepared for.

Regarding the shooting in Aurora, Colorado, when I went out afterwards and talked to the chief and our special agent in charge, the one thing they told me is: We did so well on this particular case because we trained for this before.

In Boston, if you talk to individuals such as the chief of police of the Lawson Police Department, the Cambridge Police Department, the Massachusetts State Patrol, or State Police, they will tell you that it is the collegiality, the working together on the JTTF and other areas that kicked into place when that happened on that Monday. And kudos to the first responders from Boston, the Boston Police and the others, who were responsible for security. They ran toward the danger, did not run away, and together were remarkable in the capabilities and the success they had in saving lives.

It is developing those relationships before something like this happens that is absolutely instrumental. When you have sequestration and the budget cuts that we do, what gets cut often is training. Training develops relationships that enable you to respond effectively and efficiently to something like Boston.

Chairwoman MIKULSKI. Well—and then this is going to take me to the prevention part of it. But I recall really when we were facing the sniper situation here in the North Capital Region, and the work of the FBI and Bureau of Alcohol, Tobacco, Firearms then with local law enforcement, and the fantastic job that was done. And we didn't have to "nationalize" it, though it involved two

States and multiple counties within those States; and the way everybody worked together.

I had the chance, along with then-Senator Sarbanes, to observe it very up close and personal. It was an amazing effort of coordination, where everybody was best at what they were best at, best at what they were needed for. But ultimately it was our Federal agencies that had the resources both nationally, technically through laboratories, etcetera, that we could identify it.

Now let's go to—and this will be something we'll also go into in our classified hearing, which is the resources to prevent these. I think we'll save those for the classified hearing.

But before we recess, when we think about where the FBI was on September 10, 2001, and where we are today, it has been a remarkable transformation. And it's occurred under your leadership, organizationally a phenomenal feat, and under your stewardship. You are to be commended.

My question is that, since 9–11 could you estimate how many terrorist attacks the FBI has thwarted?

Mr. MUELLER. Well, I would say over the last 3 to 4 years, it's probably close to 100 terrorist attacks, individuals who were contemplating, were involved with, or otherwise. That's just over the last 4 years. People talk about several hundred. It really depends on your definition of a terrorist attack, but I'm comfortable saying that in the last 3 to 4 years at least, we've disrupted anywhere from 90 to 100 attacks.

Chairwoman MIKULSKI. Each one of those attacks would have caused casualties, would have had a massive impact on the economy.

Mr. MUELLER. I'd say for a majority of them that is accurate. There are others that I couldn't go so far as to say that, because some of those are persons who provide material support to a terrorist attack—it's not going to be the person who punches the button.

Chairwoman MIKULSKI. You mean the enabler, the facilitator?

Mr. MUELLER. I'm sorry. Those figures are fairly accurate.

Chairwoman MIKULSKI. I note that Senator Boozman is here. Senator, we were about to recess and go into our closed hearing.

Senator BOOZMAN. Yes, ma'am. I'll ask my questions there, then. I just want to thank you for your service again, Director, for all that you've done. I know that you've worked really hard to keep us safe, so we appreciate it.

Mr. MUELLER. Thank you, Sir.

ADDITIONAL COMMITTEE QUESTIONS

Chairwoman MIKULSKI. We note that there are other Senators that are on their way. We're going to encourage them to go to the other meeting.

[The following questions were not asked at the hearing, but were submitted to the Department for response subsequent to the hearing:]

QUESTIONS SUBMITTED TO HON. ROBERT S. MUELLER, III

QUESTIONS SUBMITTED BY SENATOR RICHARD C. SHELBY

CLOSED CASE FILES

Question. With respect to closed case files on a previously investigated individual, I am interested in whether there is a process for prompting a re-investigation of that individual if they engage in any future suspicious activity—such as traveling to a region known for Islamic extremism?

If so, why did that process not occur in the case of Tsarnaev?

Answer. The FBI considers the totality of the available information, both newly acquired and within our holdings, when making the decision to initiate or re-open an investigation. Travel records are one source of information, but may not be sufficient by themselves to initiate or re-open an investigation. Due to the ongoing investigation, the FBI is unable to provide additional information specific to the Tsarnaev case.

DATABASE SEARCH

Question. In the immediate aftermath of the bombings, the FBI appealed to the public for video footage and still photos to identify a suspect. Did the FBI also return to its databases to discern whether there were any individuals in the area that had been flagged as a potential terrorist threat?

If so, did Tsarnaev turn up in that search or did he continue to elude you because the case had been closed?

Answer. The FBI has many active and closed cases involving national security. Whether a case is open or closed, the information, such as identifying information for subjects, witness statements, intelligence gathered pertaining to the case, is maintained in the FBI's databases. In the aftermath of the Boston bombings, the FBI took every step possible to identify potential subjects. However, searching FBI and Intelligence Community databases is only one tool in identifying subjects, and absent additional identifying information for the potential subjects (i.e., names, dates of birth), the decision was made in the Boston investigation to ask the public to help identify and locate the potential subjects. Due to the ongoing investigation, the FBI is unable to provide additional information specific to the Tsarnaev case.

BIG PICTURE ANALYSIS VERSUS CASE FILE MENTALITY

Question. The findings of the Joint Inquiry on September 11th, of which I was a part, identified the FBI's weaknesses with respect to intelligence analysis. They specifically noted that the FBI's "casefile mentality . . . does not generally incentivize attention to big-picture, preventive analysis and strategy." In the additional views I submitted to accompany those findings, I noted that law enforcement organizations handle information, reach conclusions, and ultimately just think differently than intelligence organizations.

In light of the Boston bombing and the gaps in intelligence that are coming to light—particularly with respect to the FBI's "closed case files", do you believe that the FBI still operates with this mentality?

Answer. No. The FBI operates as an intelligence-driven organization, with a dual national security and law enforcement mission, which is focused on stopping terrorist attacks and protecting the American public from other threats.

Question. If not, please explain the specific actions that have been taken to ensure that "big picture" capability and culture are fostered? In other words, what is the FBI doing to transition from an investigatory body to one that looks at the information as a whole, analyzes it, and uses it to close the gaps?

Answer. In response to events of 9/11 and the 9/11 Commission recommendations, the FBI transitioned from a traditional law enforcement organization to an intelligence-driven organization. As part of this transition, the FBI added hundreds of "big picture" intelligence analysts to its ranks; stood-up numerous Joint Terrorism Task Forces (JTTFs) with our Federal, State, and local partners; restructured its national security programs to attempt to ensure all the dots are connected; enhanced its human intelligence collections capabilities; worked with Intelligence Community and law enforcement partners to facilitate information sharing; furthered its foreign language and translation capabilities; and streamlined and standardized processes throughout the organization.

As an intelligence-driven organization with a dual national security and law enforcement mission, the FBI is more efficiently and effectively using intelligence to drive operations. Significant advancements have been made in many areas over the

past year to ensure the FBI is positioned to meet its missions within the constraints of budgetary reductions.

In 2012, the FBI's efforts to advance its intelligence capabilities focused on streamlining and optimizing the organization's intelligence components while simultaneously positioning the Bureau to carry out its responsibilities as the lead domestic intelligence agency. In addition to streamlining core functions and organizational structure, the FBI transferred a variety of functions including domain management, collection management, targeting, tactical analysis, strategic analysis, and finished intelligence production from the Directorate of Intelligence (DI) to intelligence personnel embedded within the FBI Headquarters (FBIHQ's) operational divisions. Realigning intelligence functions and associated resources into the operational divisions has enabled the FBI to more effectively use intelligence to drive operations.

Additionally, within the operational divisions, threat-based fusion cells serve as intelligence teams to integrate all aspects of the intelligence cycle, providing a more strategic and nimble approach to identifying and mitigating current and emerging threats. The implementation of the fusion cell model within the operational divisions also facilitates a more seamless collaboration between Intelligence Analysts and Special Agents so the organization can focus on threats and better address its priorities.

As the U.S. Government's lead domestic intelligence agency, the FBI is required to identify, prioritize, and mitigate a variety of threats impacting national interests and public safety. The FBI has developed a standardized methodology for prioritizing these threats at the national and field levels, developing a national threat picture, and effectively directing work to mitigate those threats. This process highlights emerging threats and their distribution across the Nation, which provides FBIHQ with a national threat picture.

The FBI also details numerous employees to other Intelligence Community (IC) entities and hosts detailees from many other Government agencies to foster understanding of how the Bureau contributes to the national security mission and to increase collaboration. IC detailees work alongside FBI employees and build relationships that last long after the assignment has ended.

TERRORIST EXPLOSIVE DEVICE ANALYTIC CENTER

Question. The Terrorist Explosive Device Analytic Center or TEDAC (Tea-Dak) has worked diligently since its inception to fully analyze, and exploit all terrorist improvised explosive devices, or improvised explosive devices (IEDs), found both in theater and at home. TEDAC is responsible for gathering and sharing intelligence throughout the Federal Government about these devices—helping to disarm and disrupt IEDs, link them to their makers, and most importantly, to prevent future attacks.

Given the mission of the TEDAC could you explain what role it played following the bombing in Boston? How was law enforcement able to use that information to locate those responsible for the bombing?

Answer. The FBI's Terrorist Explosive Device Analytical Center (TEDAC) deployed a team to Boston and developed a significant amount of information regarding the explosives used. Because the investigation progressed so quickly, it was not the TEDAC's efforts that led to the location of the Tsarnaev brothers. However, TEDAC is continuing to collect and process evidence from the explosions.

Question. What other benefits does the TEDAC provide to the United States in its fight against terrorism?

Answer. The Terrorist Explosive Device Analytical Center (TEDAC) was established in 2004 to serve as the single interagency organization to receive, analyze, and exploit terrorist improvised explosive devices (IEDs) of interest to the United States. TEDAC coordinates U.S. Government efforts, including law enforcement, intelligence, and military efforts, to gather and share intelligence about these devices. These efforts are designed to disarm and disrupt IEDs, link them to their makers, and prevent future attacks.

TEDAC has received tens of thousands of IEDs and related submissions, and has identified bomb makers and networks through biometrics and scientific analysis. For example, since 2003, TEDAC has shared tens of thousands of prints with its partners and has identified hundreds of individuals with potential ties to terrorism. Several individuals whose identity matched latent prints recovered from IEDs in Iraq and Afghanistan have applied for and been denied refugee status in the United States. TEDAC has also provided prosecution support to Iraq and Afghanistan in hundreds of cases and has shared thousands of boxes of IED parts and related items with other Government agencies for their own informational purposes and research.

Since April 2009, TEDAC has assisted in disrupting 31 counterterrorism plots through its explosives substitution program. The substitution program uses the surreptitious substitution of explosives, munitions/military ordnance, and blasting accessories in ongoing FBI investigations. For example, in one investigation in which TEDAC assisted, four individuals were convicted of a 2009 plot to detonate explosives near a Bronx synagogue and to attack an Air National Guard Base in Newburgh, New York. The subjects were charged with conspiring to use weapons of mass destruction within the U.S. and conspiring to acquire and use anti-aircraft missiles.

QUESTIONS SUBMITTED BY SENATOR SUSAN M. COLLINS

Question. I am particularly concerned about fraud against our seniors. I'm the ranking member of the Aging Committee and we held a hearing (March 13) on a particularly troubling scam targeting our seniors—the Jamaican Lottery scam.

Sophisticated scammers from Jamaica call and tell a victim that they've just won millions in a lottery, but they just have to pay some fees or taxes to collect their winnings. Of course, there are no winnings. These criminals are sophisticated and use various techniques to convince or threaten their victims into sending money to pay fees or taxes with the promise of lottery winnings. They spend hours on the phone with vulnerable seniors and when the victims don't cooperate, these criminals threaten their victims. In some cases, these criminals in Jamaica use satellite maps to locate and describe victims' homes in the United States to make threats. Sometimes these criminals adopt different identities to steal more money. They often pose as Federal law enforcement, including the FBI, and ask for personal information so that they "solve the crime" when the winnings do not appear and then they steal more money from these victims with this information.

Fraud against the elderly is a nation-wide problem. The FTC reported complaints from U.S. citizens regarding Jamaican lottery fraud have increased exponentially from 1,867 in 2007 to an estimated 30,000 in 2011. However, this is a seriously under-reported crime and these complaints do not accurately reflect the extent of the problem. According to a New England phone company (Fairpoint), this Jamaican lottery scam has cost Americans an estimated $300 million annually.

Some of my constituents have lost more than a hundred-thousand dollars to this scam. Others have lost their homes, their cars, and their financial independence, not to mention their security and their dignity.

I know the Jamaican Government (after years of ignoring this problem) has finally focused its attention on this problem, particularly since the U.S media began reporting on the scam late last year. I remain concerned that there is a lack of coordination by U.S. law enforcement to address this crime. Chairman Nelson and I wrote Attorney General Holder (March 15) expressing our concerns about the lack of coordination by Federal law enforcement and the need to focus on extradition of these criminals from Jamaica.

I have a constituent (Kim Nichols) whose father was a victim of these criminals. Her father lost over $85,000 to this scam from December 2001 until June 2012—when his daughter had to disconnect and change his phone number. He had been receiving 85 to 100 phone calls a day, often threatening calls. My constituent told us that she made over 100 phone calls to various law enforcement entities, including the FBI, but nobody (except the York County Maine Sheriff's Office) would help. She did tell us that she was eventually able to schedule a meeting with an FBI agent, but the agent never showed up.

My question is twofold: (1) What is the FBI doing to focus investigative resources on this scam and protect our seniors from these criminals?

Answer. The Jamaican Lottery scam is one of many Mass Marketing Fraud schemes targeting our Nation's citizens. Mass Marketing Frauds target individuals of all ages and walks of life. Victims are lured with false promises of significant cash prizes, goods, services or good works, in exchange for up-front fees, taxes or donations. Mass Marketing Fraud schemes victimize millions of Americans each year and generate losses in the hundreds of millions of dollars.

The FBI shares your concerns and works aggressively to investigate these types of fraud. The FBI does not have the resources to investigate every instance of fraud; however, at the local and national level, we participate in a number of working groups and task forces dedicated to combating significant frauds against our Nation's citizens. In an effort to optimize efficiency and effectiveness, the FBI works closely with various governmental and private entities to investigate and prevent fraudulent activity. The FBI's law enforcement and regulatory partners include the Securities and Exchange Commission, United States Attorney's Offices, United

States Commodity Futures Trading Commission (CFTC), Financial Industry Regulatory Authority (FINRA), Federal Trade Commission (FTC), United States Postal Inspection Service (USPIS), Consumer Financial Protection Bureau (CFPB), Social Security Administration (SSA), and the Internal Revenue Service, among others. The FBI's participation in interagency working groups ensures training and intelligence sharing with our international, Federal, State, and local law enforcement partners.

Specifically as it relates to fraud targeting seniors, the FBI participates in the Elder Justice Interagency Working Group, a national group that focuses on preventing, detecting, and combating frauds that harm our senior citizens. The FBI also participates in the International Mass Marketing Fraud Working Group (IMMFWG) which consists of law enforcement, regulatory, and consumer protection agencies from Australia, Belgium, Canada, EUROPOL, the Netherlands, Nigeria, the United Kingdom, and the United States. The IMMFWG seeks to facilitate a multinational exchange of information and intelligence; the coordination of cross-border operations to detect, disrupt and apprehend individuals and organizations engaged in Mass Marketing Fraud; and the enhancement of public awareness and public education measures concerning international Mass Marketing Fraud schemes.

Question [continuing]. (2) Where do these victims and their families go for help?

Answer. There are several resources that fraud victims and their families can use to seek assistance. To report a Mass Marketing Fraud, individuals and State or local law enforcement can visit the FBI tip page at www.fbi.gov or contact the nearest FBI field office. The FBI provides victim assistance and referrals to additional resources, including information about crime victims' rights, the investigative process, and ways to recover financial loss and address credit problems, through its victim specialists and at www.fbi.gov/stats-services/victim__assistance/fincrime__vic.

To combat the numerous individuals and organizations engaged in fraud who would do our citizens harm, the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) established the Internet Crime Complaint Center (IC3). IC3 (www.ic3.gov) serves as a means to receive Internet crime complaints.

The IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the Federal, State, local, and international level, the IC3 provides a central referral mechanism for complaints involving Internet related crimes. Significant and supplemental to partnering with law enforcement and regulatory agencies, it will remain a priority objective of the IC3 to establish effective alliances with industry. Such alliances will enable the IC3 to leverage both intelligence and subject matter expert resources, pivotal in identifying and in crafting an aggressive, proactive approach to combating cyber crime.

To help combat the targeting of seniors by fraudulent telemarketers, individuals are encouraged to enroll in the Federal Trade Commission's (FTC) National Do Not Call Registry. The FTC, also collects complaints about companies and business practices. The FTC enters all complaints received into Consumer Sentinel, a secure online database used by thousands of civil and criminal law enforcement authorities worldwide. A complaint can be submitted at www.ftccomplaintassistant.gov or through a toll-free Consumer Help Line, 1–877–FTC–HELP (1–877–382–4357). Fraud complaints submitted to IC3 are automatically submitted to the FTC's Consumer Sentinel.

Information related to common white-collar scams and tips to help prevent individuals from being victimized can be found on the FBI website at www.fbi.gov. For additional tips on how to spot investor scams and for more information on investor fraud in general, please visit www.stopfraud.gov or www.lookstoogoodtobetrue.com.

Question. Director Mueller, I would like to ask you a question about the role the Bureau is expected to play in the investigation of the emerging IRS scandal.

A report released by the Treasury Inspector General for Tax Administration (TIGTA) shows that the IRS targeted groups critical of the Government or that worked to educate the American people about the Constitution and the Bill of Rights. Also troubling are reports that the IRS sought to compel the targeted groups to divulge their membership lists. Lois Lerner, the director of exempt organizations division, has admitted that there was no reason for the IRS to have sought this type of information, and that it was not appropriate for the IRS to have done so. Thus, the fact that the IRS chose to press these organizations for their membership lists suggests an effort to chill the constitutional rights of speech and association by groups that hold conservative views and that were seeking tax-exempt status.

The FBI is the lead Federal agency for investigating color of law abuses, which include acts carried out by Government officials operating both within and beyond the limits of their lawful authority. Preventing the abuse of that power is essential to the health of our democracy. Federal law contains several provisions making clear that Federal officials who act under "color of law" to willfully deprive or conspire to deprive a person of a right protected by the Constitution or U.S. law would be committing a crime, including title 18, sections 241 and 242.

Do you believe that "color of law" statutes in the U.S. Code apply to the Internal Revenue Service?

Answer. As the Attorney General has previously stated, DOJ and FBI are reviewing IRS's actions to determine if there was a violation of Federal criminal law, including whether there has been any violation of title 18 U.S.C. section 241 (conspiracy to injure, oppress, threaten, or intimidate the free exercise of any right secured by the Constitution or Federal law) and/or section 242 (deprivation of rights under color of law).

Question. Will the Bureau participate in the investigation of the IRS?

Answer. Yes. As the Attorney General has previously stated, DOJ and FBI are reviewing IRS's actions to determine if there was a violation of Federal criminal law.

QUESTIONS SUBMITTED BY SENATOR MARK KIRK

Question. Chicago currently has the highest per capita of gang violence in the country. I am extremely concerned about the loss of life we are experiencing and the violence on the streets of Chicago.

How much money in your fiscal year 2014 budget request is devoted to fighting gangs nationwide? And how to do you make decisions on the regional allocation of the money?

Answer. The fiscal year 2014 request to Congress includes 497 positions (420 Agents) and $102 million to investigate gang related crime. The regional allocation of funding is assessed throughout the year and is based on open investigations in each field office.

Question. Your fiscal year 2014 budget justification seems to indicate that the FBI will target "dismantling" significantly fewer gangs than in previous years, down to 99 in fiscal year 2014 from 163 in fiscal year 2012. Is this correct? Why are you targeting almost 40 percent fewer gangs than you dismantled in fiscal year 2012 and fiscal year 2011?

Answer. The target number for gang dismantlements set by the FBI does not stop the FBI from dismantling additional gangs during the fiscal year once the target is met, as evidenced by the number of dismantlements in fiscal year 2012. In that year, the target was also 99 dismantlements and the actual number of dismantlements was much higher, at 163. The FBI did not revise is fiscal year 2014 target downward from prior years.

Question. What Federal resources are available to assist our State and local law enforcement to fight gangs?

Answer. The Department of Justice has a variety of tools to assist our State, local, and tribal law enforcement partners in fighting violent gangs. The Department recognizes violent gangs as among the most significant criminal threats that we face, and that it is vital to partner with Federal, State, local, and tribal law enforcement to leverage resources to combat the threat.

As part of this effort, the FBI's Safe Streets Violent Crime Initiative was created in 1992 to establish FBI sponsored, long-term, proactive task forces focusing on violent gangs, crimes of violence, and the apprehension of violent fugitives. These Violent Gang Safe Street Task Forces (VGSSTFs) expand cooperation and communication amongst Federal, State, and local law enforcement agencies, increasing productivity and avoiding duplication of investigative efforts. There are approximately 160 VGSSTFs nationwide, staffed by 839 FBI agents, 1,588 State and local law enforcement personnel (1,411 full-time and 177 part-time task force officers), and 92 other Federal law enforcement agents. ATF, DEA, and USMS also participate in task forces with State and local law enforcement throughout the country to help fight gang-related crime. Through these task forces, DOJ agencies share with State and local law enforcement their unique expertise and leverage Federal resources such as the National Integrated Ballistic Information Network (NIBIN) and firearms tracing to help link shooters to violent crimes and their firearms sources.

One example of the success the FBI has had working with State and local partners regarding violent gangs is the Save Our Streets efforts in Chicago, which the FBI participated in from September 2012 to January 2013. This effort was in re-

sponse to the high rate of homicides, shootings and gang violence taking place in Chicago, and was coordinated with the Chicago Police Department. FBI Chicago's efforts resulted in the initiation of at least 16 new FBI cases, the development of 11 new Confidential Human Sources, 68 arrests, 30 violent crime matters solved or advanced through investigation, the seizure of 61 firearms, the prevention of seven violent incident crimes, and seizures of marijuana, crack cocaine and heroin.

The centerpiece of the Office of Justice Programs (OJP's) efforts to address youth violence is the National Forum for Youth Violence Prevention (Forum). This program creates a context for participating localities to share challenges and promising strategies with each other and to explore how Federal agencies can better support local efforts. It brings together groups across the spectrum, including, local and Federal leaders, law enforcement, educators, public health providers, community and faith-based representatives, parents, and young people to share ideas about effective and affordable ways to prevent youth and gang violence. In fiscal year 2010 and fiscal year 2011, the Forum sites developed comprehensive, multi-strategy plans to address youth violence in their cities. Boston, Chicago, Detroit, Memphis, Salinas, and San Jose have come together with national and local leaders to more effectively identify needs, and target scarce resources in the most violent areas in their cities. The Department of Justice and the Department of Education have supported this initiative by forging a relationship with numerous Federal agencies and through coordinated technical assistance to the sites. For example, this technical assistance has come in the form of: training on how best to collect and analyze data; best practices for addressing truancy; coalition building; strategic planning to address serious violence; addressing youth gangs; developing coordinated management information systems; and a "toolkit" to assist any interested locality in developing and implementing comprehensive youth violence prevention plans on their own. In fiscal year 2012, the Forum expanded from six sites to ten. Camden, New Jersey, Minneapolis, Philadelphia, and New Orleans were competitively selected to join the Forum and will complete their comprehensive youth violence prevention plans in the summer of 2013. These additional resources will be utilized in support of the existing sites and as a means to share the experiences of the Forum cities with other communities across the nation that are struggling with the issue of youth violence.

Finally, OJP's Community-Based Violence Prevention Initiative funds programs that adopt a comprehensive public health approach to investigate the causes of youth violence and implement a community-based strategy to prevent youth violence by addressing both the symptoms and causes of neighborhood violence. The Community-Based Violence Prevention Initiative assists localities, and/or State programs that support a coordinated and multi-disciplinary approach to gang prevention, intervention, suppression, and reentry in targeted communities. This initiative aims to enhance and support evidence-based direct service programs that target both youth at-risk of gang membership, as well as, gang involved youth. Additionally, this initiative will support programs that reduce and prevent other forms of youth violence through a wide variety of activities such as street-level outreach, conflict mediation, and the changing of community norms to reduce violence, particularly shootings.

Question. I am aware of various task forces that exist to fight gangs, including the Violent Gang Safe Streets Task Forces. How much money is being requested in this budget for these types of task forces? How are you working to ensure that these task forces are not duplicating the work of other agencies such as DEA?

Answer. Funding for the VGSSTFs is primarily derived from the Department's Assets Forfeiture Fund (AFF). Typically, the AFF provides approximately $25 million to support 160 VGSSTFs throughout the country. When VGSSTFs Task Force Officer costs (such as overtime, fuel, vehicles) exceed the AFF allotment in any given year, the FBI utilizes its direct budget to cover these costs. In fiscal year 2012, FBI used an additional $5.5 million from its direct appropriation, to complement the $22 million provided in AFF funding. We anticipate a similar funding requirement in fiscal year 2014.

The FBI works diligently to ensure our VGSSTFs are not duplicating efforts of other Federal agencies, and utilizes existing national, regional and local deconfliction centers to foster collaboration between law enforcement entities. These centers are used to deconflict investigative data and target information, which permits agents to identify potentially overlapping investigative efforts. These platforms also permit for the deconfliction of law enforcement events, which enhances officer safety by preventing the occurrence of "blue-on-blue" episodes. Presently, the Department is exploring the implementation of a single platform point of access to these deconfliction systems, the DICE/DART platform, for all Department law enforcement agencies, which will facilitate the usage of these deconfliction methods. While the technical aspects of a single platform point of access are being considered,

the Attorney General Anti-Gang Coordination Committee (AGCC) continues to ensure that task forces are not duplicating one another. Department policy requires all new task forces proposed by DOJ components to first be considered and approved through the AGCC, which considers, among other factors, whether the threat to be addressed is already being addressed by another law enforcement task force or initiative in the same area. Finally, the Department calls upon its United States Attorneys to convene regular forums with their Federal, State, and local law enforcement partners to foster and enhance coordination and information sharing on a more localized level. By bringing together high-level commanders with decisionmaking authority (e.g., Special Agents-in-Charge, Assistant Special Agents-in-Charge, U.S. Marshals and Chief Deputy Marshals, and State and Local Police Chiefs, Commanders, and Captains) for those areas most in need, and by providing an environment that encourages an open exchange of information and ideas, United States Attorneys can assist the collective group to develop and design a sustainable anti-violence strategy, and provide a valuable mechanism for deconfliction and elimination of duplicated efforts. The Department reiterated this message and strongly encouraged its United States Attorneys to convene such forums in a memorandum to all United States Attorneys dated August 12, 2013.

Question. The FBI's fiscal year 2014 budget proposes eliminating the National Gang Intelligence Center (NGIC). How to you propose to handle the work that is currently performed by the NGIC if it is eliminated? Your budget request states, "the FBI will continue to produce intelligence products in support of Federal, State, and local investigations." Will additional funds be needed in other accounts to produce these products? If not, how will they be paid for?

Answer. Given budget constraints, the FBI must prioritize its programs. If the NGIC program is eliminated in fiscal year 2014, the FBI will adjust its remaining resources to ensure continued intelligence sharing on gang-related matters.

QUESTIONS SUBMITTED BY SENATOR FRANK R. LAUTENBERG

Question. While full details of the attacks are not yet known, the recent bombings in Boston have highlighted dangerous loopholes in our explosives laws. Today, anyone can buy up to 50 pounds of black powder and unlimited quantities of smokeless and black powder substitute without a background check or permit.

Do you think these loopholes in our explosives laws put Americans' safety in danger?

Answer. The Department's focus is enforcing current laws and investigating the misuse of explosives purchased legally and the use of explosives procured illegally. Nevertheless, the Department is open to discussions regarding ways to potentially strengthen existing law to better prevent the criminal or terrorist use of explosives.

Question. In June 2011, Adam Gadahn, an American-born Al Qaeda member, urged terrorists in a video to exploit weaknesses in U.S. gun laws to carry out terrorist attacks. Gadahn said, "America is absolutely awash with easily obtainable firearms. You can go down to a gun show at the local convention center and come away with a fully automatic assault rifle, without a background check, and most likely, without having to show an identification card. So what are you waiting for?"

Do you believe there are loopholes in our gun laws that put our national security at risk?

If so, please identify those loopholes.

Answer. The FBI's focus is on enforcing current laws. The Department of Justice fully supports the President's gun safety initiatives announced in January, including expanding the number of firearms transactions subject to a background check to prevent firearms reaching persons prohibited from obtaining them. The Department looks forward to continuing a dialogue with Congress on this proposal and other ways to strengthen gun safety legislation.

Question. Even when a background check is conducted, being a known or suspected terrorist does not disqualify a person from purchasing a gun or acquiring an explosives permit/license. While we don't yet know how the Boston bombing suspects acquired a firearm, reports indicate that Tamerlan Tsarnaev was added to at least one terror watch list/database at the request of the Central Intelligence Agency.

What terror watch databases/lists, if any, was Tamerlan Tsarnaev on?

Answer. The response to this inquiry is classified.

Question. Please identify the various databases/lists that identify known or suspected terrorists.

Answer. The Terrorist Screening Database (TSDB) is the U.S. Government's consolidated terrorist watchlist on Known or Suspected Terrorists (KSTs). Once accept-

ed into TSDB, records are, as appropriate, exported to screening agency systems for use in their operations. The most common screening systems are:

—Department of Homeland Security TECS;
—Department of State Consular Lookout And Support System (CLASS);
—National Crime Information Center (NCIC) Known and Suspected Terrorist File (KSTF);
—Transportation Security Administration (TSA) Secure Flight; and
—Select Foreign Partners.

Question. Of these lists, which ones are queried during a firearm sale conducted by a Federal Firearms Licensee and during the application for an explosives permit/license?

Answer. TSDB data exported to NCIC–KSTF is used to screen firearms purchases through the National Instant Criminal Background Check System (NICS).

Question. Would the Attorney General having the discretionary authority to deny the sale of a firearm to a known or suspected terrorist help the FBI prevent terrorist attacks?

Answer. Under current Federal law, there is no basis to automatically prohibit a person from possessing firearms or explosives, for being a known or appropriately suspected terrorist. If legislation should be proposed in this regard, we would be pleased to provide our views to the Department of Justice (DOJ) pursuant to DOJ's role in assisting in the development of the Administration's position.

Question. A recent Department of Justice statutory ruling determined that individuals who come to the United States under the Visa Waiver Program are legally permitted to purchase guns in this country.

Are foreign fugitives or foreign felony and domestic violence misdemeanor convictions identified during a background check conducted during a firearm sale by a Federal Firearms Licensee?

Answer. The NICS responds to each background check query with all available information matched (by name and descriptor) to records available in the following three national databases:

—The Interstate Identification Index (III), which contains criminal history records provided by local, State, tribal, and Federal agencies;
—The National Crime Information Center (NCIC), which provides records such as foreign fugitives, criminal warrants, protection orders, etc.; and,
—The NICS Index, which houses firearm-prohibiting information provided by state and Federal agencies. These records contain information about persons who are prohibited from the purchase/possession of firearms of which the prohibiting information is not maintained in the III or the NCIC, e.g., a felony indictment/information, disqualifying mental health record, etc.

Some foreign conviction information is contained in III and NCIC. However, foreign convictions do not qualify as Federal firearms prohibitions. Several States have State prohibitions for foreign convictions. Due to this, foreign convictions are eligible for entry into the NICS Index. Foreign conviction records in the NICS Index would only be returned during a firearms background check if specific State prohibiting criteria exists.

Also, a search of the applicable databases of the Department of Homeland Security's U.S. Immigration and Customs Enforcement is requested by the NICS, and is conducted for all prospective firearm transferees who claim non-U.S. citizenship on the ATF Form 4473. Foreign criminal history records not available in the aforementioned databases are not checked.

Question. Similarly, does a NICS background check identify mental illness adjudications conducted in foreign countries?

Answer. The NICS does not have access to mental health adjudications from other countries.

Question. As you know, I have long advocated for restricting the size of high-capacity magazines. Also, the President's plan to reduce gun violence called for limiting high-capacity gun magazines to 10 rounds.

Does a criminal having to reload his firearm slow down a shooter?

If so, does a criminal reloading allow victims a greater opportunity to escape and make it easier for law enforcement to intervene?

Answer. Any disruption in a shooter's firing might help victims to flee and help victims and law enforcement officials to intervene. The degree to which this is helpful will depend on the length of the disruption and the other circumstances involved.

Question. Do you think banning the manufacture, sale, importation, and transfer of magazines carrying more than 10 rounds is in the best interest of the public?

Answer. The FBI works to enforce the laws passed by Congress. The Department of Justice supports the President's gun safety initiatives, including reinstating the prohibition on ammunition magazines holding more than 10 rounds.

Question. According to the FBI, New Jersey is home to the most at-risk area for a terrorist attack in the United States. An attack on this area could have an impact on 12 million people who live nearby. Last year, you assured me that the FBI continues to dedicate critical investigative resources to New Jersey's high-risk areas.

What specific items in this budget request will help the FBI protect this area?

Answer. The FBI has a Field Office in Newark, New Jersey and five Resident Agencies throughout New Jersey that are responsible for 18 of New Jersey's 21 counties. Camden, Gloucester, and Salem counties fall within the territory of the Philadelphia Field Office.

Resources:

—Fiscal year 2012 actuals: 658 employees (353 Agents, 54 Intelligence Analysts, 251 Professional Staff) and $89,564,000 (personnel and non-personnel)
—Anticipated fiscal year 2013 investment: 660 employees (353 Agents, 54 Intelligence Analysts, 253 Professional Staff) and $89,381,000 (personnel and non-personnel)
—The fiscal year 2014 President's budget supports a comparable level of investment.

Recent Operational Outcomes: The following represents a sample of the operational outcomes that the Newark Field Office contributed to between June 2012 and June 2013.

—On June 5, 2013, U.S. Attorney Paul Fishman announced that Duy Hai Truong, one of the leaders of an international data theft ring, was charged with his alleged role in a scheme which caused approximately $200 million in fraudulent charges to credit cards issued in the U.S. and Europe.

Duy Hai Truong, 23, of Ho Chi Minh City, Vietnam, was charged by criminal complaint with conspiracy to commit bank fraud. From 2007 until his arrest, Truong allegedly defrauded financial institutions as part of the massive scheme, in which personal identifying information relating to more than 1.1 million credit cards was stolen and resold to criminal customers worldwide.

Global law enforcement efforts by the FBI, the United Kingdom's Serious Organized Crime Agency (SOCA) and Vietnamese authorities disbanded the ring following a worldwide investigation into Truong and his conspirators. Truong was charged in the United States in conjunction with charges and arrests made in the United Kingdom, Vietnam, Italy, Germany and elsewhere.

—On May 13, 2013, the central organizer of a worldwide conspiracy to manipulate stock prices through a "botnet" network of virus-controlled computers was sentenced in Trenton Federal court to 71 months in prison.

Christopher Rad, 44, of Cedar Park, Texas, was previously convicted, following a 9-day jury trial, of six counts arising from the fraud scheme: conspiring to further securities fraud using spam; conspiring to transmit spam through unauthorized access to computers; and four counts of transmission of spam by unauthorized computers.

This investigation was part of efforts underway by President Obama's Financial Fraud Enforcement Task Force (FFETF), which was created in November 2009 to wage an aggressive, coordinated and proactive effort to investigate and prosecute financial crimes. With more than 20 Federal agencies, 94 U.S. Attorneys' offices and State and local partners, it is the broadest coalition of law enforcement, investigatory and regulatory agencies ever assembled to combat fraud. Since its formation, the task force has made great strides in facilitating increased investigation and prosecution of financial crimes; enhancing coordination and cooperation among Federal, State and local authorities; addressing discrimination in the lending and financial markets and conducting outreach to the public, victims, financial institutions and other organizations.

—On March 25, 2013, a former New Jersey-based defense contractor employee who was convicted by a Federal jury for exporting sensitive U.S. military technology to the People's Republic of China (PRC), stealing trade secrets and lying to Federal agents was sentenced to 70 months in prison.

In 2010, Sixing Liu, aka, "Steve Liu," 49, a PRC citizen who had recently lived in Flanders, New Jersey, and Deerfield, Illinois, stole thousands of electronic files from his employer, L–3 Communications, Space and Navigation Division, located in Budd Lake, New Jersey. The stolen files detailed the performance and design of guidance systems for missiles, rockets, target locators and unmanned aerial vehicles. Liu stole the files to position and prepare himself for future employment in the PRC.

—On January 7, 2013, Michael Rumore, an attorney formerly licensed in New Jersey, was arrested in connection with a long-running, large-scale mortgage fraud scheme which caused losses of more than $30 million.

From September 2006 to May 2008, Rumore and the other defendants engaged in a long-running, large-scale mortgage fraud conspiracy through a mortgage company called Premier Mortgage Services ("PMS"). The conspirators targeted properties in low-income areas of New Jersey (the "subject properties"). After recruiting "straw buyers," the defendants used a variety of fraudulent documents to make it appear as though the straw buyers possessed far more assets, and earned far more income, than they actually did. The defendants then submitted these fraudulent documents as part of mortgage loan applications to financial institutions.

Relying on these fraudulent documents, financial institutions provided mortgage loans for the subject properties. The defendants then split the proceeds from the mortgages among themselves and others by using fraudulent settlement statements ("HUD–1s"), which hid the true sources and destinations of the mortgage funds provided by financial institutions.

—On November 16, 2012, an associate of two lead defendants in a racketeering case was sentenced to 6 months in prison for providing them with ammunition despite knowing they were both convicted felons.

—On September 6, 2012, a Newark, New Jersey man was sentenced to 66 months in prison for his role in a $40.8 million mortgage fraud conspiracy, recruiting "straw buyers" to purchase real estate properties in New Jersey, South Carolina, and Georgia and causing lenders to release more than $18 million based on fraudulent mortgage loan applications.

—On August 10, 2012, a former Newark resident, who earlier in the year was extradited from Nigeria, admitted his role in a scheme to use stolen identities to loot retirement accounts.

Rasheed Mustapha, 35, who used to live in Newark, and his conspirators gained access to seven different 401(k) retirement accounts using confidential customer identity information. Mustapha stole this information through his employment as a customer service representative at a Little Falls, New Jersey, call center for the retirement accounts. After taking over the accounts, Mustapha and others tried to clean them out by having rollover checks issued, mailed to members of the conspiracy, and deposited into bank accounts they controlled under various aliases in New Jersey, Pennsylvania, Georgia and Arizona.

—On August 2, 2012, an executive with global pharmaceuticals giant Bristol-Myers Squibb Co. was arrested on insider trading charges related to illegal trades he made based on information concerning three BMS acquisition targets.

—On June 20, 2012, a Passaic County man who is a member of the Bloods street gang was sentenced to 89 months in prison for his role in a racketeering conspiracy that included violent crimes and narcotics distribution.

Michael McCloud, a/k/a "Ike Brim," 26, of Paterson, a member of the Fruit Town Brims (FTB) set of the Bloods, admitted to selling crack cocaine to an undercover officer on August 30, 2006, together with two other members of the gang. McCloud also admitted to participating in two robberies in Paterson in 2006. McCloud was involved in the robbery of a dice game in Paterson, in which a co-conspirator used an AK–47 and the gang members took controlled substances, cell phones, and money. He also conspired with other FTB members to commit a robbery, also involving a gun, in retaliation for the shooting of an FTB member by a member of a rival gang.

Question. Crime onboard cruise ships continues to be a serious problem. Outside of U.S. waters, passengers onboard cruise ships do not have the same protections as on land in the U.S. The FBI plays an important role in protecting passengers by investigating crimes and reporting the number of crimes that occur. Frequently, the FBI is the only investigative entity that victims have access to.

Are all serious crimes onboard cruise ships reported to the FBI?

Answer. The Cruise Vessel Security and Safety Act of 2010 (CVSSA) requires cruise lines to report allegations of all serious crimes (sexual assault, kidnapping, tampering with the vessel, homicide, suspicious death, theft greater than $10,000, missing U.S. National) to the FBI if they meet the reportable criteria under the law. The cruise lines send a written report of the serious allegation to FBI Headquarters and contact the nearest FBI field office or Legal Attach by email or telephone.

Question. In what instances would the FBI not find out about a serious crime onboard a cruise ship?

Answer. The CVSSA requires serious crimes to be reported if they meet one of the following requirements: (1) the vessel is owned, in whole or in part, by a U.S.

person and the incident occurs when the vessel is within the admiralty and maritime jurisdiction of the U.S. and outside the jurisdiction of any other country; (2) the incident concerns an offense by or against a U.S. person committed outside the jurisdiction of any nation; (3) the incident occurs in U.S. territorial waters; or (4) the incident concerns a victim or subject who is a U.S. national on a vessel that departed from or will arrive at a U.S. port.

Based on the above criteria, one example of a scenario that would not require FBI notification would be: a foreign national subject allegedly sexually assaults a foreign national victim on a cruise departing/returning to Barcelona, Spain and the incident occurs in non-U.S. territorial waters.

Question. How does the FBI determine which cases to investigate?

Answer. The FBI reviews the facts of all alleged serious crimes by conducting interviews of the victim and alleged subject(s), and collecting physical evidence. The relevant U.S. Attorney's Office (USAO) determines if there is sufficient evidence to seek a prosecution of the subject(s). Examples where prosecution may be declined by the USAO include, but are not limited to, circumstances in which there is late notification to the FBI and evidence has been substantially compromised by the delay.

Question. What happens to the cases that are not investigated?

Answer. Cases that are not investigated by the FBI may be referred to a State or local law enforcement agency if venue is established and a violation of State or local law has occurred. Cases that are not referred are closed.

Question. Does the FBI analyze cruise crime data to determine which vessels or cruise lines have patterns of crimes onboard?

If so, what recourse does the FBI have to address those patterns?

Answer. The FBI does not analyze cruise crime data to determine which vessel or cruise lines have patterns of crimes onboard.

Question. In the instances where the FBI has access to video surveillance onboard cruise ships, is it able to provide that surveillance to victims of crime?

Answer. Any video surveillance of a crime would be considered evidence of that crime. Typically, a victim of a crime will not be shown video surveillance of the crime so as not to influence the victim's recollection of the crime.

Question. Since 2001, terrorist attacks against mass transit, buses, and passenger rail have resulted in 3,900 deaths and 14,000 injuries worldwide. Rail and transit systems in the U.S. have received heightened attention, as several terrorists' plots have been uncovered, including attempts to attack systems in the New York City and Washington, D.C. areas. Most recently, on April 22, 2013, a plot to attack the Canadian Via transit agency with service into New York City was uncovered, and the FBI was the lead U.S. agency investigating this plot with the Canadian Government.

Given the FBI's role in investigating transit and passenger rail security threats, what additional steps could be taken to secure these systems against future attacks?

Answer. The FBI has investigated and will continue to investigate threats related to transit and passenger rail security. However, the Department of Homeland Security (DHS) is the agency responsible for protection of transportation infrastructure in the United States. The FBI will continue to convey threat information to partners, including DHS, so adequate steps can be implemented to thwart and mitigate threats.

Question. Only one person has ever been convicted in connection with the Pan Am 103 bombing, and that person has since been released from prison. On February 28, 2012, then Secretary of State Hillary Clinton testified that the U.S.'s ongoing investigation into the bombing is primarily the responsibility of the FBI and the Department of Justice. However, the FBI and DOJ have refused to provide any updates on the investigation.

Does the FBI still consider the investigation into the bombing of Pan Am 103 to be active?

Answer. The FBI continues to work diligently with intelligence and law enforcement partners in order to bring each of the Pam Am Flight 103 Bombing suspects to justice. However, the Department of Justice and FBI have long-standing policies not to release information of an ongoing investigation. These policies have existed for a number of years and serve to protect the rights of all parties involved. The FBI appreciates your concern in this matter and regrets that we are unable to provide any additional information.

Question. What progress has been made on this bombing investigation?

Answer. The FBI continues to work diligently with intelligence and law enforcement partners in order to bring each of the Pam Am Flight 103 Bombing suspects to justice. However, the Department of Justice and FBI have long-standing policies not to release information of an ongoing investigation. These policies have existed

for a number of years and serve to protect the rights of all parties involved. The FBI appreciates your concern in this matter and regrets that we are unable to provide any additional information.

Question. What resources, including personnel, has the FBI committed to investigating the Pan Am 103 bombing?

Answer. The FBI continues to work diligently with intelligence and law enforcement partners in order to bring each of the Pam Am Flight 103 Bombing suspects to justice. However, the Department of Justice and FBI have long-standing policies not to release information of an ongoing investigation. These policies have existed for a number of years and serve to protect the rights of all parties involved. The FBI appreciates your concern in this matter and regrets that we are unable to provide any additional information.

Question. What challenges has the FBI faced in its investigation of this terror attack?

Answer. The FBI continues to work diligently with intelligence and law enforcement partners in order to bring each of the Pam Am Flight 103 Bombing suspects to justice. However, the Department of Justice and FBI have long-standing policies not to release information of an ongoing investigation. These policies have existed for a number of years and serve to protect the rights of all parties involved. The FBI appreciates your concern in this matter and regrets that we are unable to provide any additional information.

Question. Super Bowl XLVIII will be held on February 2, 2014 in New Jersey. While the investigation into the April 15, 2013 bombings at the Boston Marathon continues, these attacks highlight the terrorist threat posed to large sporting events. For many years, the FBI, in conjunction with the Department of Homeland Security, has noted that mass gatherings continue to remain attractive terrorist targets. The ability to inflict mass casualties and cause massive economic damage at an event of national importance has made high-profile sporting events a target around the globe for terrorist attacks.

How is the FBI working with the Department of Homeland Security, the National Football League, and State and local law enforcement officials to coordinate security for Super Bowl XLVIII?

Answer. The FBI, through the Critical Incident Response Group, Special Events Management Unit (SEMU) has been engaged in the deliberate Counterterrorism/Domestic Preparedness planning effort for Super Bowl XLVIII since March of 2012. The Chief of SEMU is a Co-Chair of the Special Events Working Group, a United States Government interagency group, managed by the Department of Homeland Security, which provides Federal level oversight and policy for the planning and support to major events domestically. These events range from locally managed events where limited Federal support is required to major events drawing significant international media coverage such as the Super Bowl and where the full support of the Federal Government is applied in support of our state, local and private sector partners.

The initial step taken to ensure the FBI was fully engaged and supporting this high profile event was to deliver comprehensive briefings to the local Newark and New York offices of the FBI which addressed the FBI's responsibilities for Counterterrorism, Domestic Intelligence Collection, Crisis Management, Bomb Management, Weapons of Mass Destruction and Hostage Rescue/Tactical response. These briefings were followed by interagency briefings with State, local and private sector stakeholders (NFL) associated with the safe delivery of the games to discuss roles, responsibilities and obligations across the various echelons of government. The FBI also provided operational briefings concerning the establishment of an Executive Steering Committee, the functional Sub-Committees, and the planning structures, templates, timelines and best practices developed from prior Super Bowls.

Since these initial briefings, SEMU has assigned two Special Events Planners from the unit to work full time with the Newark and New York FBI field offices to assess capabilities, identify short falls, and to coordinate Federal support to fill these identified gaps. This planning effort will result in a formal Operations Order issued by the Special Agent in Charge of the Newark Field Office and will also be incorporated into the DHS Integrated Federal Support Overview for Super Bowl XLVIII.

SEMU has also assessed the internal capabilities of the local FBI offices and is currently working with the Newark FBI office to design, build, and equip an interagency Intelligence Operations Center and Joint Operations Center which will be used as a multi-agency command and control platform during the event. These centers will provide situational awareness at the local and national command level and will address threat related issues, or in the event of a critical incident, operate as the focal point for all case related activity.

SUBCOMMITTEE RECESS

Senator MIKULSKI. This subcommittee will recess and we'll reconvene in the Capitol Visitors Center, where we can proceed with the security brief, and then some of the other questions that Senators—Senator Collins, we're about to go over to our classified briefing. Did you want to ask a question here or can it wait until we go over there?

Senator COLLINS. It can wait if you would prefer.

Chairwoman MIKULSKI. Let's recess, go over there, and you have—your time will be reserved, along with Senator Boozman. We know that there were many hearings.

The subcommittee is in recess. We'll reassemble in CVC 217.

[Whereupon, at 10:53 a.m., Thursday, May 16, the subcommittee was recessed, to reconvene in closed session.]